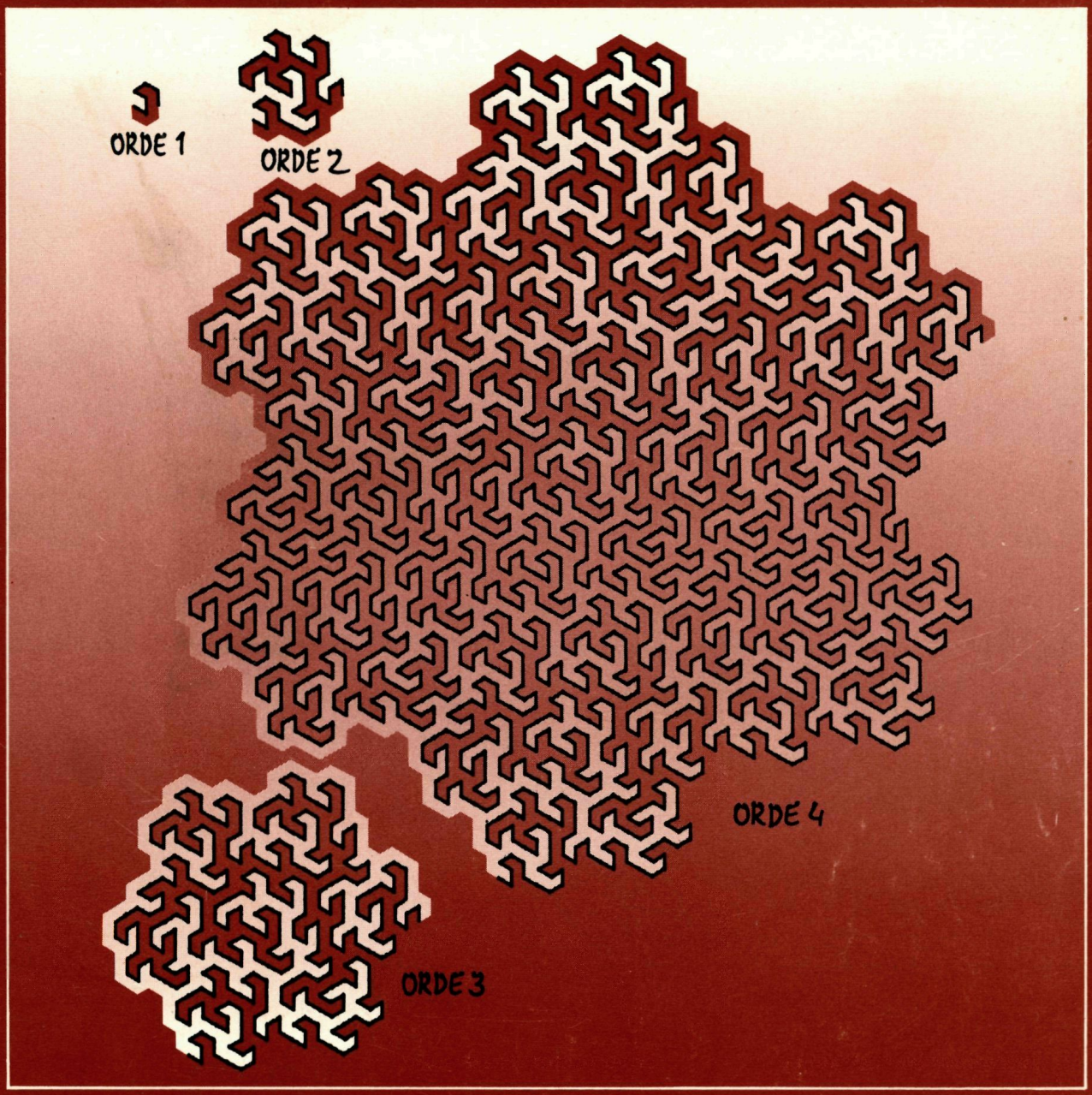


Verschijnt vier keer per jaar

Wiskundetijdschrift voor jongeren

Pythagoras

4 Jaargang 24 mei 1985

Wolters-Noordhoff

Pythagoras

Dit tijdschrift wordt uitgegeven onder auspiciën van de Nederlandse Onderwijscommissie voor Wiskunde.

Redactie Jan van de Craats, Luc Kuijk, Klaas Lakeman, Henk Mulder, Hessel Pot, Hans de Rijk, Leo Wiegerink

Secretariaat Leo Wiegerink, Egelantiersstraat 107^{II} 1015 PZ Amsterdam

Illustraties Evert Gerardts

Foto's Theo van de Rakt, Oss: pag. 75

Inhoud

Pythagoras verschijnt 4 maal per schooljaar.
Voor leerlingen van scholen, collectief besteld via één der docenten, f 9,95 (Bfr 185) per jaargang.
Voor anderen f 15,05 (Bfr 275).

Abonnementen kan men opgeven bij:
Wolters-Noordhoff bv, Afdeling Periodieken,
Postbus 567, 9700 AN Groningen.
Voor België bij: J.B. Wolters-Leuven,
Blijde Inkomststraat 50, Leuven;
postchecknummer 000-000 8081-38.
Abonnees wordt dringend verzocht met betalen te wachten tot een acceptgirokaart wordt gezonden.

Bij de voorplaat Zeshoek-figuren van ordes 1, 2, 3 en 4. Wanneer je deze figuren door een computer wilt laten tekenen, moet je precies uitzoeken hoe elke figuur is opgebouwd uit *zeven* deelfiguren van één orde lager en *zes* verbindingsstreepjes. De 0-de orde figuur bestaat slechts uit een verdraaiing over 60° (met de klok mee) van de pen-richting! Hoe zoiets in z'n werk gaat lees je in het artikel 'Tekenen met de computer'.

Eerlijk met binnenbaan en buitenbaan

Een mens kan een galopperend paard bijhouden en dat gaat behoorlijk snel, zo'n 35 km per uur. Natuurlijk houdt de mens dit niet zo lang vol als het paard. Dat kunnen we zien als we de gemiddelde snelheden op de diverse loopnummers uitrekenen. Doen de heren-atleten over de 100 meter minder dan 10 seconden, gemiddelde snelheid 36 km per uur, op de 10 km wordt een tijd van 27 min 30 s gehaald, wat neerkomt op een gemiddelde snelheid van 21,8 km per uur. Die gemiddelde snelheid is op de marathon (42,195 km in 2 uur 8 min) afgenomen tot 19,7 km per uur. Nog niet slecht als je de afstand in aanmerking neemt: als eenvoudig fietser zul je flink door moeten trappen wil je dit halen.

Van de marathon wordt altijd een officieuze tijd gegeven, omdat er niet op een atletiekbaan wordt gelopen. Voor alle officiële afstanden van 100 meter tot en met 10 km zijn er reglementen die bepalen hoeveel ronden er gelopen dienen te worden, in welke baan en vanaf welk punt er gestart moet worden. Deze reglementen schrijven voor dat bij de wedstrijdafstanden 100, 200 en 400 meter de deelnemers in naast elkaar gelegen, eigen banen lopen. De officiële benaming voor baan luidt: 'laan'. Een atletiekbaan heeft zes of acht lanen. Bij de 400 meter loopt de loper in de binnenlaan precies één rondje en het is zonder meer duidelijk dat de hardlopers in de naar buiten gelegen lanen dus minder dan één volledige ronde moeten lopen!

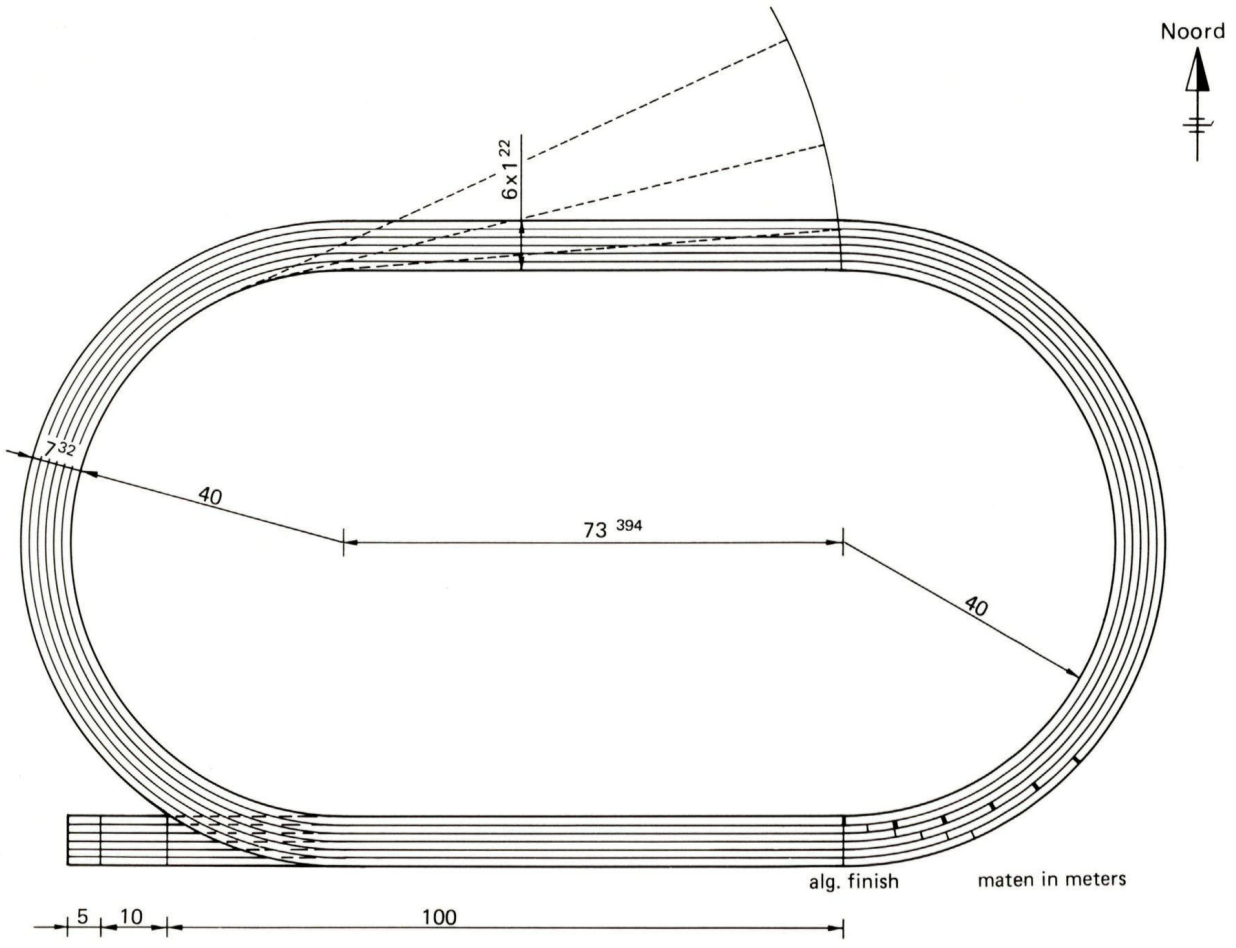
Voor lopers, publiek en jury (tijdwaarneming!) is het plezierig als de finish een rechte eindstreep is. Dit betekent dat de startlijnen ten opzichte van elkaar verschoven moeten worden: de lopers in de buitenlanen krijgen een zogenaamde voorgift, die zo berekend is dat ieder precies 400 meter gelopen heeft als hij of zij over de eindstreep gaat. Iedere loper moet daarbij in zijn laan blijven.

Standaard atletiekbaan (6-laans). Uitgezet zijn alle lijnen en afstanden voor de 100 meter, 400 meter en 800 meter hardlopen. De dikke startstrepen zijn die van de 400 meter, de dunne die van de 800 meter. De kromme lijn direct na de eerste bocht is een evolvente (afwikkelkromme) van de cirkel gevormd door de tweede binnenbocht. Vanaf die lijn mogen de lopers bij de 800 meter naar de binnenste laan en is het voor elke loper nog even ver naar de finish.
Om te laten zien hoe de evolvente ontstaat, is hij verlengd tot buiten de baan: de stippellijnen zijn als het ware touwtjes in diverse posities, die strak om de tweede bocht liggen.
(Gegevens in dit artikel werden ons verstrekt door de Technische Commissie van de Nederlandse Sport Federatie. Er wordt daar behalve aan sport ook veel aan wiskunde gedaan!)

V

Hoe nauwkeurig?

Tegenwoordig kunnen de tijden met de elektronische tijdwaarneming in hondersten van een seconde nauwkeurig gemeten worden. Als we uitgaan van een gemiddelde snelheid van 10 m/s op de 400 meter, betekent dit dat in een honderdste van een seconde 1 decimeter wordt afgelegd. Om deze reden worden alle afstanden op de 400-m-baan zó nauwkeurig uitgezet dat eventuele afwijkingen minder dan 5 cm zijn. Twee verschillende 400-m-banen wijken dan minder dan die 1 decimeter van elkaar af!
Om de vereiste nauwkeurigheid te halen worden alle maten tot op de millimeter opgegeven. Vandaar dat je in dit artikel ook alle afstanden (die in meters gegeven worden) in drie decimalen nauwkeurig vindt.



De 400 meter

Op de bladzijde hiernaast is zo'n 400-m-baan weergegeven. Het is er een met 6 lanen. We zullen voor elke laan de voorgift berekenen.
De lengte van het lange rechte stuk is 73,394 m. De straal van de twee halve cirkels is precies 40 m (tot aan de binnenkant).
De lengte van de binnenomtrek is dus:
$2\pi \times 40 + 2 \times 73{,}394 \approx 398{,}115$ m (met $\pi = 3{,}14159\ldots$).
Dat is dus nog geen 400 meter, er ontbreken nog bijna 2 meter. Hoe dat zit?
Heel eenvoudig: men gaat er terecht van uit dat de binnenste loper niet precies op de binnenrand (een witte rechtopstaande richel!) loopt, maar 30 cm ervandaan. Hij loopt dus in werkelijkheid:
$2\pi \times 40{,}300 + 2 \times 73{,}394 \approx 400{,}000$ meter!
De andere lopers lopen niet langs een opstaande richel, maar langs een witte streep met een breedte van 5 cm. En er is experimenteel vastgesteld dat ze daar zo'n 20 cm vanaf lopen. Als je verder nog weet dat elke laan 1,220 m breed is (inclusief de streep aan de rechterkant) dan kun je dus nagaan dat de halve cirkels voor de tweede loper als straal hebben: $40 + 1{,}220 + 0{,}200 = 41{,}420$ m, zodat een rondje $2\pi \times 41{,}420 + 2 \times 73{,}394 \approx 407{,}038$ m lang is. De loper in de tweede laan krijgt dan ook een voorgift van 7,038 m!
Voor elke volgende loper worden de stralen van de halve cirkels weer 1,22 m groter, zodat een heel rondje steeds $2\pi \times 1{,}220 \approx 7{,}665$ m groter wordt. Dat is dus de voorgift die elke loper krijgt op de loper een laan meer naar binnen!
Wil je zelf de voorgiften uitrekenen bij een 8-laans baan, dan zijn daarvoor de volgende gegevens beschikbaar:
lengte rechte stuk: 84,390 m
straal halve cirkels: 36,500 m
breedte van een laan: 1,255 m

De 800 meter

Voor de 800 meter liggen de berekeningen geheel anders. Dat komt doordat de lopers direct na het uitkomen van de eerste bocht naar de binnenste laan mogen lopen.

Wereldrecords hardlopen

mannen			
100 m	9,93s	Smith (VS)	Col. Springs 1983
400 m	43,86s	Evans (VS)	Mexico City 1968
800 m	1m 41,72s	Coe (GB)	Florence 1981
10 km	27 m 22,4s	Rono (Kenia)	Wenen 1978
marathon	2 u 8m 13s	Salazar (VS)	New York 1981
vrouwen			
100 m	10,79s	Ashford (VS)	Col. Springs 1983
400 m	47,99s	Kratochvilova (CSSR)	Helsinki 1983
800 m	1m 53,28s	Kratochvilova (CSSR)	München 1983
10 km	31m 27,57s	Safrefolmova (USSR)	Odessa 1983
marathon	2u 22m 43s	Benoit (VS)	Boston 1983

Misschien heb je wel eens opgemerkt dat na de eerste bocht een vloeiende kromme op de baan getrokken is. Dat is de lijn waarvandaan de lopers naar die binnenste laan mogen. En die lijn is een heel bijzondere wiskundige kromme: een zogenaamde *afwikkelkromme* of *evolvente*.

Evolvente

Stel je eens voor dat langs de tweede binnenbocht (preciezer: weer 30 cm van de rand) een touw strak tot het einde van de eerste bocht is gespannen.
Precies langs de weg van de binnenste loper dus! We trekken nu in gedachten dat eindpunt van het touw naar buiten, zodat het touw strak om de tweede bocht blijft liggen. Het eindpunt beschrijft dan een kromme lijn: de afwikkelkromme of evolvente van de cirkel die door de tweede bocht gevormd wordt.
Vanaf die evolvente moet elke loper precies evenveel meters afleggen naar de finish. Waarom? Denk maar aan dat denkbeeldige touw! De voorgiften moeten nu dus zó groot zijn dat elke loper ook tot die evolvente een even grote afstand aflegt, ieder natuurlijk in zijn eigen laan.
Je zult wel begrijpen dat de juiste bepaling daarvan nogal wat rekenwerk vergt, waar o.a. de vergelijking van de evolvente een rol in speelt. Er zullen ongetwijfeld lezers zijn die de berekening aandurven en ook tot een goed einde weten te brengen. Zij kunnen

hun uitkomsten vergelijken met wat wij er zelf uitkregen:

laan	voorgift
1	0,000 m
2	3,528 m
3	7,388 m
4	11,270 m
5	15,171 m
6	19,092 m

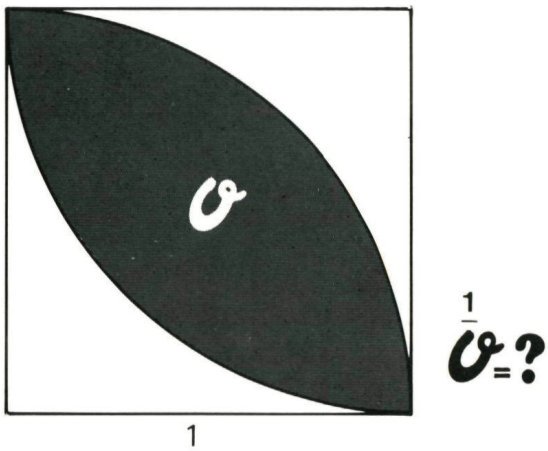
Andere baanvormen

Hoe zit het nu met binnenbaan en buitenbaan op circuits van minder eenvoudige vorm, zoals bijvoorbeeld in de figuur hiernaast?
Op het eerste gezicht lijkt dit een moeilijke vraag. Het antwoord is echter verrassend eenvoudig. *De voorgiften zijn precies als op een gewone atletiekbaan!* Mits de baanbreedte daarmee overeenstemt. Wie kan dat verklaren?

Nog verrassender: op 'acht-achtige' banen zijn voorgiften helemaal overbodig, omdat alle lanen precies even lang zijn! Is dat een idee voor de Nederlandse Sport Federatie?
Die ongelijkvloerse kruising mag toch geen probleem zijn!

O-tjes

Dit keer een nummer vol oppervlakte-sommetjes, oplopend van gemakkelijk tot moeilijk. Om de figuren zo mooi mogelijk te houden hebben we rechte-hoek tekentjes weggelaten. Maar alles wat er als vierkant of rechthoek uitziet, is ook als zodanig bedoeld!
Op bladzijde 95 kun je je oplossingen controleren.



Van de uitgever

Graag hadden wij het volgend jaar de 25e jaargang van Pythagoras uitgegeven. Maar helaas is het abonneeaantal de laatste jaren te klein geworden. Daarom heeft Wolters-Noordhoff besloten Pythagoras niet langer uit te geven.
Veel mensen hebben zich jarenlang ingespannen om Pythagoras tot een succes te maken. We bedanken al die mensen hartelijk voor de kwaliteit van het gebodene, voor hun inzet en enthousiasme en voor de goede samenwerking.

De uitgever

Dit trieste bericht bereikte de redactie tijdens haar werkzaamheden aan dit nummer. Waarschijnlijk heb je het al via de krant vernomen, want er is zo hier en daar nogal wat aandacht aan besteed. Het zou het einde kunnen betekenen van Pythagoras, hetgeen algemeen en niet in de laatste plaats door de redactie als een groot verlies wordt gezien voor wiskundig Nederland.
We zijn echter niet bij de pakken neer gaan zitten en stellen alles in het werk om Pythagoras alsnog op een of andere manier te kunnen laten verschijnen. Degenen die menen ons daarbij te kunnen helpen, kunnen zich wenden tot Pythagoras, Cornelis Krusemanstraat 60II, 1075 NS Amsterdam. Wie weet, komt er straks in september toch nog een feestelijke 25e jaargang.
Graag willen we van onze kant dank uitbrengen aan de mensen van Wolters-Noordhoff voor de wijze waarop zij vierentwintig jaar lang de uitgave van dit blad mogelijk hebben gemaakt. Het is jammer dat daar een einde aan moest komen, maar we hebben daar alle begrip voor.
Verder willen we van de gelegenheid gebruik maken om alle leraren en abonnees te danken voor het vertrouwen dat ze in ons blad hebben gesteld. We hopen dat we bij een eventueel vervolg van Pythagoras weer op ze mogen rekenen.

De redactie

Correspondentie

Uitslag geheimschrift

In deze jaargang hebben we veel aandacht besteed aan geheimschrift. Het eerste artikel daarover in nummer 1 van deze jaargang eindigde met een stuk cijfertekst dat je zelf kon gaan ontcijferen. We vertelden daarbij dat je inspanningen zeker niet voor niets zouden zijn. Degenen die aan de slag gegaan zijn hebben dan ook ontdekt dat ze te maken hadden met een ceasaralfabet met een verschuiving van 10 en de volgende klare tekst verkregen:

Wanneer je dit hebt ontcijferd, kun je de oplorring naar het redactiesecretariaat sturen. Je dingt dan mee naar een leuke verrassing.

Inderdaad, als je het goed gedaan had, kreeg je 'oplorring'. Er was namelijk een foutje in de opgave geslopen!
Die leuke verrassing bestond uit het boek **'Van telraam tot microcomputer'** geschreven door Ben Paul en Klaas Lakeman. Uit de vele goede inzenders die daar naar konden dingen, heeft het lot *Bettina Reinhartz*, leerlinge uit A6 van de Christelijke SG de Vlietschans te Leiden, als de gelukkige aangewezen. Zij heeft inmiddels een speciaal exemplaar van dit boek toegezonden gekregen.
Een aantal inzenders had ook zelf een cijfertekst in elkaar gezet. Bij sommigen zat die cijfertekst ingenieus in elkaar, bij anderen kwam er weer een verrassend leuke klare tekst te voorschijn. We hadden al die vondsten hier graag gepubliceerd, maar werden helaas gedwongen daarvan af te zien. Misschien komt het er nog wel eens van.

Gelijke som, gelijk product Ook hadden we wel wat meer aandacht willen besteden aan de inzending van *Jardena Gil*, leerlinge uit de derde klas van het Stedelijk Gymnasium te Utrecht, die ons verraste met vele series drietallen met gelijke som én gelijk produkt (zie nummer 2 van deze jaargang). Haar langste serie begon met het drietal (288,2210,2530) waarna nog acht drietallen volgden met dezelfde som en hetzelfde produkt.

Nogmaals gelijke som, gelijk produkt

In nummer 2 van deze jaargang werd gevraagd naar series getallen met allemaal dezelfde som én allemaal hetzelfde produkt. We dachten dat het niet zo eenvoudig was om dergelijke series te vinden. Tot onze grote verbazing vonden we echter in een boekje over rekenraadsels ook zulke series, maar dan ineengevlochten tot één groot magisch vierkant! Dit 8 bij 8 vierkant zie je hieronder staan. Alle rijen, alle kolommen en de beide diagonalen hebben alle achttien een som 840 en bovendien nog allemaal hetzelfde produkt. We konden het zelf pas geloven nadat we het helemaal hadden gecontroleerd – en nu maar hopen dat er bij het drukken geen foutje in gekomen is.

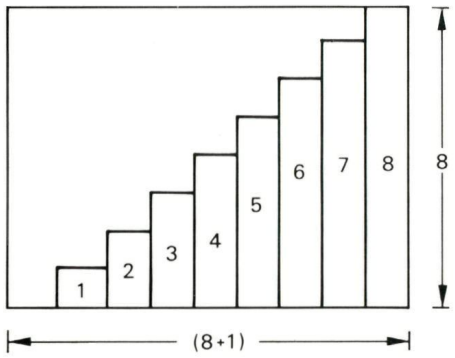
46	81	117	102	15	76	200	203
19	60	232	175	54	69	153	78
216	161	17	52	171	90	58	75
135	114	50	87	184	189	13	68
150	261	45	38	91	136	92	27
119	104	108	23	174	225	57	30
116	25	133	120	51	26	162	207
39	34	138	243	100	29	105	152

Waarschijnlijk zie je nogal op tegen dat controleren. Het optellen is nog wel te doen, maar het vermenigvuldigen lijkt een veel lastiger karwei. Het produkt wordt een getal van zestien cijfers, veel te groot voor je rekenmachine. Het is echter helemaal niet nodig om zo'n produkt helemaal 'uit te cijferen': veel handiger is het om alle getallen van het vierkant in kleinste factoren te ontbinden en dan de produkten van die ontbindingen te vergelijken. Voor elke rij, kolom en diagonaal hoort het te zijn:
$2^7 \cdot 3^8 \cdot 5^3 \cdot 7 \cdot 13 \cdot 19 \cdot 23 \cdot 29$

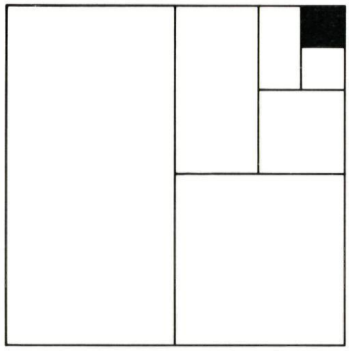
Plaatjes bij rijen

Wist je dat je formules voor de som van een getallenrij vaak kunt aantonen met behulp van plaatjes?
Hier volgen er een aantal.

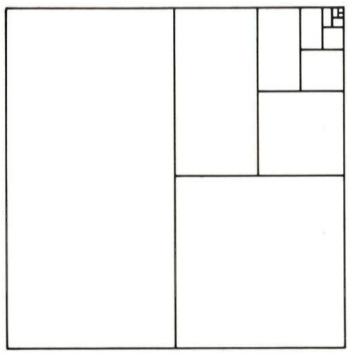
$1 + 2 + 3 + 4 + \ldots + n = \frac{1}{2}n\,(n + 1)$



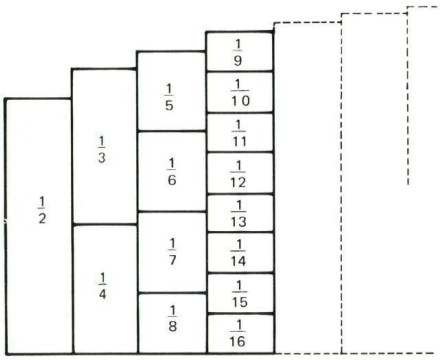
$1 + 2 + 4 + \ldots + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1$



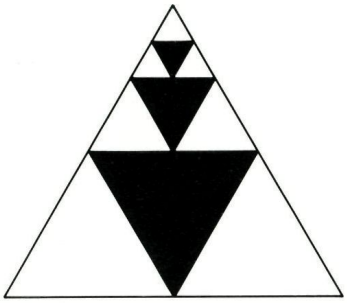
$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots = 1$



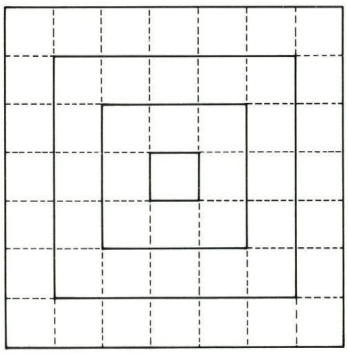
$\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \ldots = \infty$ (oneindig!)



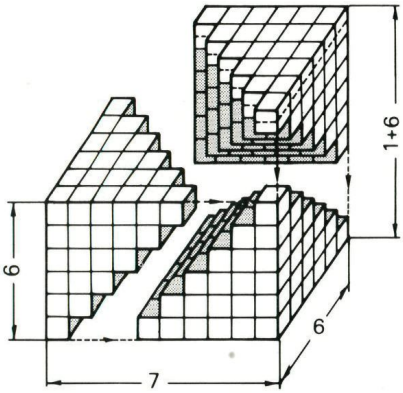
$\frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \ldots = \frac{1}{3}$



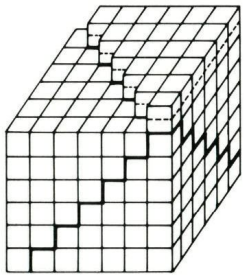
$$1 + 8 + 16 + 24 + \ldots + n \cdot 8 = (2n + 1)^2$$



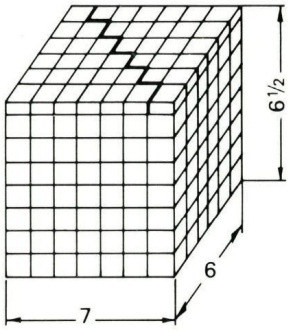
$$1^2 + 2^2 + 3^2 + 4^2 + \ldots + n^2 = \tfrac{1}{3}\, n\, (n + \tfrac{1}{2})\, (n + 1)$$



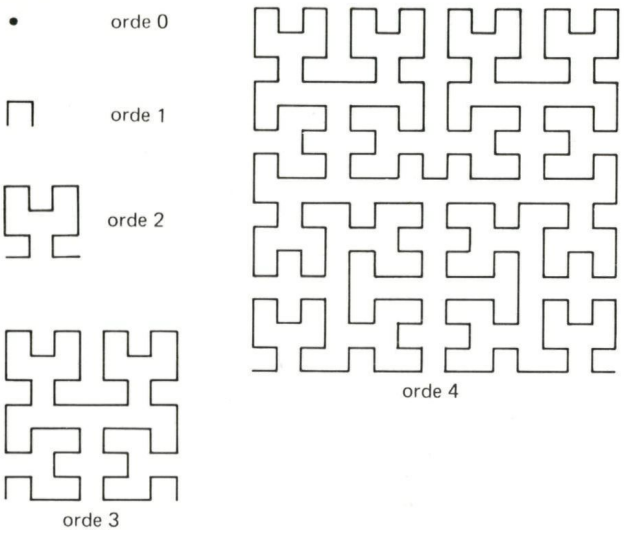
a



b



c



Tekenen met de computer

De tekeningen hierboven zijn met behulp van de computer gemaakt. Ze heten 'Peano-figuren', naar de wiskundige Peano die aan het eind van de vorige eeuw leefde. De eerste 'tekening' is slechts een los punt! Elke Peano-figuur ontstaat uit de vorige volgens een vaste afspraak. Zie je de samenhang al? Zou je de Peano-figuur van orde 3 uit je hoofd kunnen natekenen? En kun je voorspellen hoe de Peano-figuur van orde 5 er uit zal zien?

We vragen dat niet zomaar voor de aardigheid of om je bezig te houden, maar omdat de samenhang tussen de tekeningen verrassend eenvoudig is, en de basis vormt voor een eenvoudig computer-tekenprogramma. Wanneer je het principe begrijpt, kun je er daarna eindeloos op variëren. Het is natuurlijk leuk als je de tekeningen echt zelf kunt maken, bv. met behulp van de computertaal LOGO, maar nodig is het niet: ook zonder computer of programmeerkennis is de nu volgende beschrijving te volgen. Het gaat ons er vooral om te laten zien hoe hele eenvoudige opdrachten tot een resultaat leiden waarvan je zegt: 'Hoe is het mogelijk?'.

Slechts twee opdrachten

Voor het maken van dit soort tekeningen heb je slechts twee soorten opdrachten nodig:

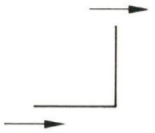
1. Opdrachten om de tekenpen een stuk lijn te laten tekenen (bv. 2 cm vooruit);
2. Opdrachten om de richting van de tekenpen te veranderen (bv. 90° linksom of 90° rechtsom).

Aan de pen moet je daarbij denken als aan een tekenapparaatje dat met z'n 'neus' een bepaalde kant opstaat.

Laten we eens een serie opdrachten bekijken, een serie die een 'hoek' tekent:

```
"HOEK"
1   vooruit
90° linksom
1   vooruit
90° rechtsom
```

Met 1 centimeter als lengte-eenheid is het resultaat:



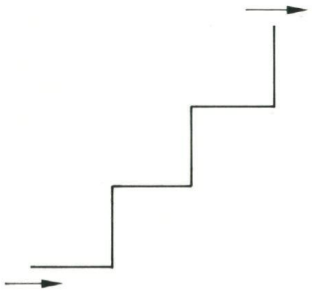
De kleine pijltjes geven de richting van de tekenpen aan, aan het begin en aan het einde. Die laatste draai rechtsom wordt van belang wanneer je de tekenopdracht laat herhalen, of inpast in een grotere tekenopdracht.

Bijvoorbeeld:

```
"TRAPPETJE"
HERHAAL
3 keer: Hoek
```

geeft het resultaat op de volgende pagina.
Ga maar na!

(Wat zou het resultaat zijn geweest als die laatste 90° rechtsom was weggelaten?).



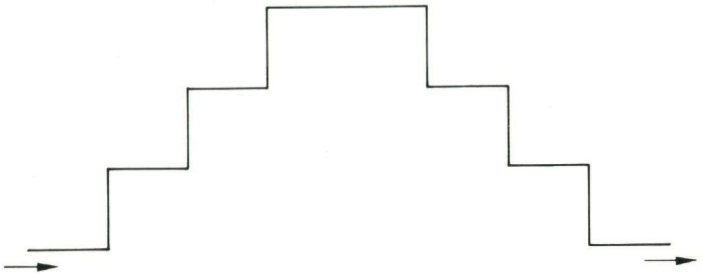
Nog een voorbeeld:

'GEVELTJE'
HERHAAL 3 keer: Hoek
2 vooruit
90° rechtsom
HERHAAL 3 keer: Hoek
90° linksom

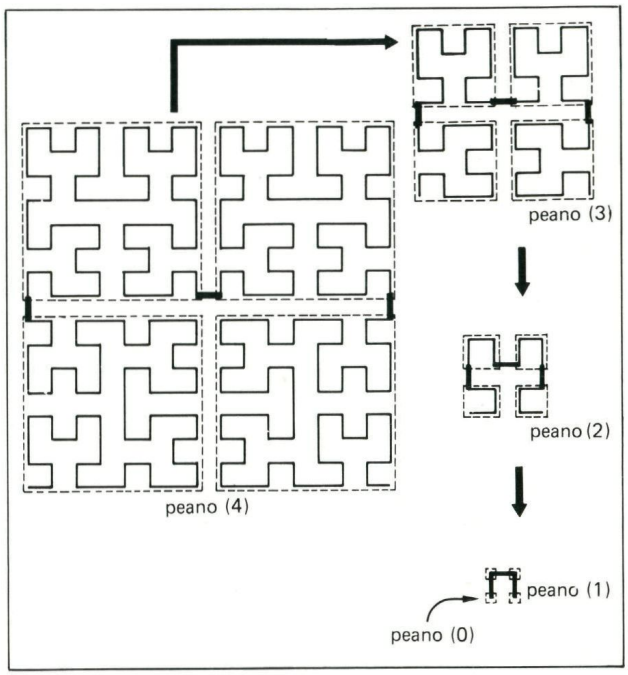
ofwel:

'GEVELTJE'
Trappetje
2 vooruit
90° rechtsom
Trappetje
90° linksom

tekent:



Welke tekenvoorschriften horen nu bij de Peano-figuren? We kijken eerst nog eens naar hun onderlinge samenhang: elke Peano-figuur bestaat uit *vier* Peano-figuren van een orde lager, met *drie* verbindingsstreepjes. Bijvoorbeeld is Peano(4) opgebouwd uit vier Peano(3)-figuren, elk in een bepaalde stand getekend, en verbonden door drie streepjes.
Op hun beurt bestaan al die Peano(3)'s weer uit vier Peano(2)'s, met drie verbindingsstreepjes.
En de Peano(2)'s? Precies, die bestaan elk weer uit vier Peano(1)'s, met drie verbindingsstreepjes.
En nog gaat het verder! Want elke Peano(1) bestaat uit vier Peano(0)'s (d.w.z. vier punten!) met drie verbindingsstreepjes!



Elke Peano-figuur is opgebouwd uit vier Peano-figuren van één orde lager met drie verbindingsstreepjes.

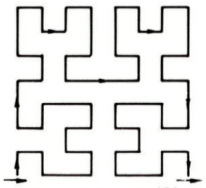
In het algemeen kun je zeggen dat voor elk getal n (met $n \geqslant 1$) de Peano(n)-figuur is opgebouwd uit vier Peano($n-1$)-figuren met drie verbindingsstreepjes! En dat is de basis van al zulke tekenprogramma's. De computer daalt om Peano(4) te tekenen net als wij af naar het laagste nivo, en tekent eigenlijk alleen maar verbindingsstreepjes tussen Peano-figuren van ordes 3, 2, 1 en 0.

Vooruit en achteruit

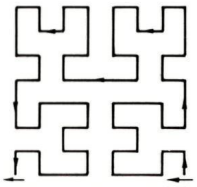
Zo, nu weet je een beetje welke kant we op willen, en kunnen we een volgende stap zetten op weg naar het tekenvoorschrift. Twee dingen moet je daarbij goed in de gaten houden:

1. Twee van de vier bij elkaar horende Peano-figuren worden 'van voor naar achter' doorlopen, en de andere twee 'van achter naar voren'!
2. De penrichting voor en na het voltooien van iedere deel-figuur is natuurlijk van groot belang om de tekening niet te laten ontsporen!

Van elke Peano-figuur maken we daarom twee varianten, een 'vooruit'-figuur en een 'achteruit'-figuur. Bijvoorbeeld:



Peano vooruit (3)



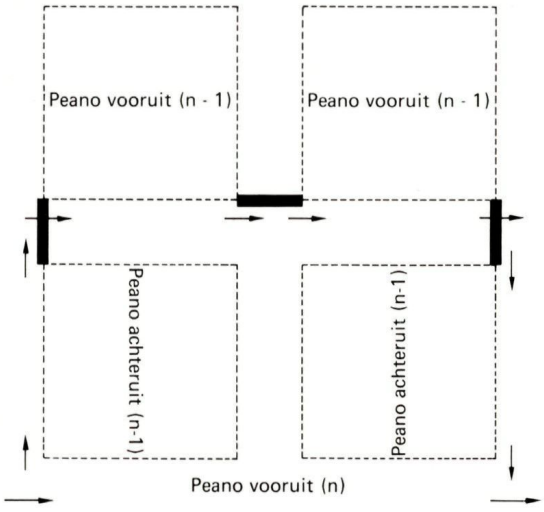
Peano achteruit (3)

Elke Peano-figuur kan 'vooruit' of 'achteruit' getekend worden: Peanovooruit(n) en Peanoachteruit(n). De tekenvoorschriften gaan uit van de aangegeven beginrichtingen van de tekenpen en stellen deze aan het einde weer net zo in.

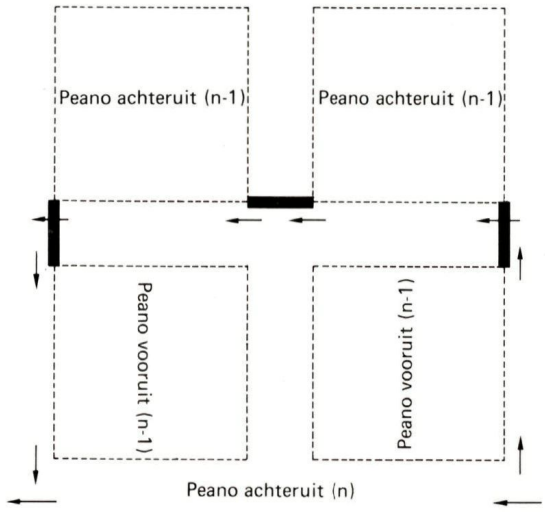
De onderste pijltjes geven een voorgeschreven begin- en eindrichting van de tekenpen, zodat altijd duidelijk is in welke richting een volgende tekenopdracht wordt uitgevoerd.
De plaatjes hieronder geven schematisch aan hoe zowel Peanovooruit(n) als Peanoachteruit(n) zijn opgebouwd uit vier deelfiguren Peano($n-1$). De figuren zelf zowel als hun deelfiguren zijn voorzien van de voorgeschreven begin- en eindrichting van de tekenpen.
En dit is de basis van het tekenschema waarmee wij en de computer het tekenen van elke Peano-figuur kunnen reduceren tot het tekenen van de Peano-figuur van een orde lager en van de bijbehorende verbindingsstreepjes (en uiteindelijk tot het tekenen van *alleen maar verbindingsstreepjes!*).
Met het vingertje bij de figuren kun je zo nagaan dat de tekenschema's voor willekeurige Peanovooruit(n) en Peanoachteruit(n) als volgt luiden:

PEANOVOORUIT(n)
ALS n=0 : teken niets!
EN ANDERS:
90° linksom
Peanoachteruit(n-1)
1 vooruit
90° rechtsom
Peanovooruit(n-1)
1 vooruit
Peanovooruit(n-1)
90° rechtsom
1 vooruit
Peanoachteruit(n-1)
90° linksom

PEANOACHTERUIT(n)
ALS n=0 : teken niets!
EN ANDERS:
90° rechtsom
Peanovooruit(n-1)
1 vooruit
90° linksom
Peanoachteruit(n-1)
1 vooruit
Peanoachteruit(n-1)
90° linksom
1 vooruit
Peanovooruit(n-1)
90° rechtsom



De tekenvoorschriften Peanovooruit(n) en Peanoachteruit(n) zijn opgebouwd uit vier Peano(n-1)-figuren waarvan er twee vooruit en twee achteruit doorlopen worden.



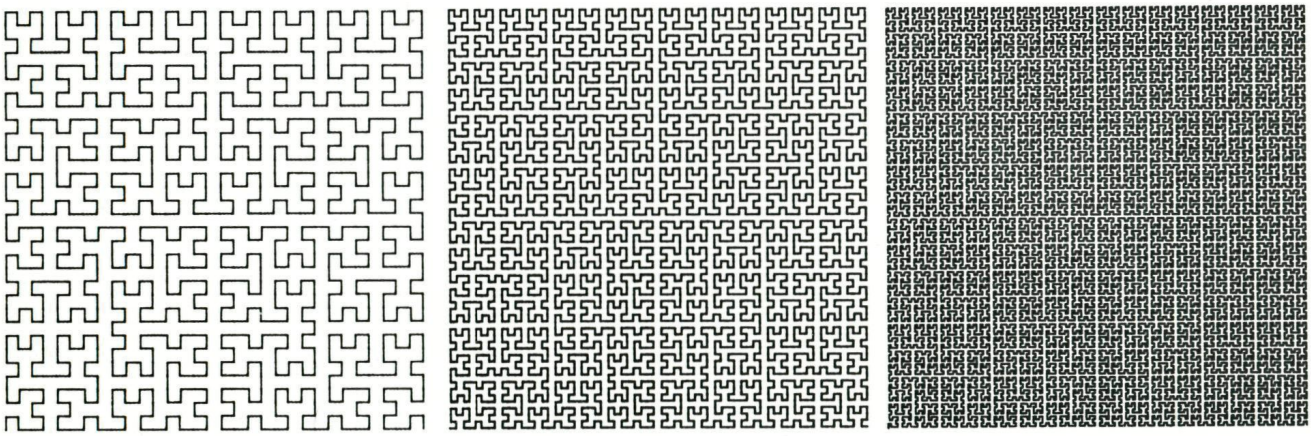
Wat doet de computer nu als hij bv. Peanovooruit(4) moet tekenen op grond van deze tekenschema's?
Wel, hij vult voor n de waarde 4 in, en voert de opdrachten in volgorde uit. Hij komt al snel Peanoachteruit(3) tegen. Hij onthoudt nu waar hij gebleven is in Peanovooruit(4) en begint bovenaan het schema Peanoachteruit(n), nu met $n = 3$. Daarin komt hij Peanovooruit(2) tegen en begint daaraan, terwijl hij onthoudt waar hij was gebleven in Peanoachteruit(3). In Peanovooruit(2) komt hij weer Peanoachteruit(1) tegen, en daarin Peanovooruit(0). Dat is 'niets' tekenen! (Eigenlijk zou het een punt moeten zijn, maar bij alle streepjes die straks komen is dat natuurlijk niet van belang). Nu neemt hij de draad weer op in Peanoachteruit(1): hij tekent eindelijk het eerste streepje(1 vooruit). Dan volgt een Peanoachteruit(0), niets dus, gevolgd door het tweede streepje van Peanoachteruit(1). Na het derde streepje, voorafgegaan en gevolgd door een Peano(0) is Peanoachteruit(1) voltooid! Dan wordt de draad weer opgepakt in Peanovooruit(2): weer een verbindingsstreepje, nu met de daarop volgende Peanovooruit (1). Zo verder tot heel Peanovooruit(2) is voltooid. De draad wordt dan weer opgenomen in Peanoachteruit(3): een verbindingsstreepje gevolgd door een Peanoachteruit(2).
En zo steeds maar verder. En alle getekende verbindingsstreepjes (1 vooruit) vormen de uiteindelijke figuur! Centraal hierbij staat het feit dat de computer inderdaad precies bijhoudt waar hij gebleven is, wanneer hij uit 't schema wegspringt om opnieuw te beginnen voor een lagere n-waarde. Je ziet dat $n = 0$ dient als de noodzakelijke stopwaarde die het almaar weer doorverwijzen onderbreekt, zodat er met '1 vooruit' ook eens wat getekend wordt!

Recursieve procedures

Zo'n tekenvoorschrift, dat onderdeel zou kunnen zijn van een computerprogramma heet een *procedure.* Natuurlijk moet het voorschrift nog in een geschikte computertaal opgeschreven worden (bv. in LOGO, of in een taal die een teken-apparaat kan besturen). Dat is eigenlijk een kleinigheid t.o.v. het verzinnen van de tekenschema's! De tekenprocedures Peanovooruit(n) en Peanoachteruit(n) hebben als bijzonderheid dat ze *elkaar* aanroepen, met een waarde van n die 1 kleiner is. Zoiets noemt men *recursie.* Een procedure die zichzelf aanroept heet een *recursieve procedure,* en twee procedures die elkaar aanroepen heten *wederzijds recursief.* Om te voorkomen dat het zichzelf of elkaar aanroepen eindeloos doorgaat, heeft elke recursieve procedure een stop-waarde. Hier is dat dus de waarde $n = 0$!

Peano-figuren van hogere orde

Hieronder zie je de Peano-figuren van orde $n = 5$, 6 en 7. Ze zijn allemaal even groot getekend, wat te bereiken is door de lengte-eenheid aan te passen aan de waarde van n.
(De ideeën voor dit artikel werden aangedragen door een lezer, Oskar van Deventer uit Eindhoven.)



Geheimschrift IV

Moderne cryptografie

Hoe kun je vertrouwelijke berichten zo vercijferen dat ze veilig verzonden kunnen worden (bijvoorbeeld via een openbaar kanaal of een telefoonlijn die afgeluisterd wordt)?
Dat is het kernprobleem van de moderne cryptografie. Veilig wil zeggen dat een onbevoegde ('de vijand') er geen kennis van kan nemen, zelfs niet als hij de vercijferde tekst onderschept of steelt. Het zou ook mooi zijn als de vijand een 'valse' boodschap niet voor echt kan laten doorgaan. Dus als hij niet aan onze tekst kan knoeien zonder dat we het in de gaten hebben.
Wat er ook mee te maken heeft, is de kwestie van de betrouwbare 'handtekening'. Hoe weet je of een bericht echt afkomstig is van degene waarvan je denkt dat het komt? Is er een soort 'elektronische handtekening' mogelijk?
Een handtekening heeft ook nog een andere functie. Je maakt er documenten *rechtsgeldig* mee. Als jouw handtekening onder een contract staat, ben je er aan gebonden; je kunt later niet ontkennen dat je het contract hebt gesloten. Een bericht of stuk met jouw handtekening eronder bewijst dus dat het van jou afkomstig is, *zelfs al zou je dat later willen ontkennen.* Denk maar eens aan koopcontracten of kwitanties. Kan dat ook allemaal met elektronische handtekeningen?

Public Key Cryptosystems

In 1976 is er door de Amerikanen Diffie en Hellman een methode bedacht waarbij gebruikers van bepaalde cryptosystemen hun berichten inderdaad kunnen voorzien van een elektronische handtekening. We zullen het principe van dergelijke Public Key Cryptosystems (openbare sleutel cryptosystemen) bespreken.

Alle berichten worden eerst, bijvoorbeeld via de ASCII-code, in getallencode omgezet. Die getallen worden vervolgens door de computer met behulp van sleutels vercijferd en eventueel weer ontcijferd.
Iedere gebruiker G van het systeem krijgt twee sleutels (per gebruiker verschillend): een *openbare sleutel* S_G en een *privé sleutel* T_G.
De openbare sleutels worden allemaal gepubliceerd in een *sleutelboek*; dat is net zo iets als een telefoonboek. Iedereen houdt z'n privé sleutel geheim, intern in het geheugen van z'n computer of op een magneetkaartje.
Elk sleutelpaar (S_G, T_G) heeft verder de volgende eigenschappen:

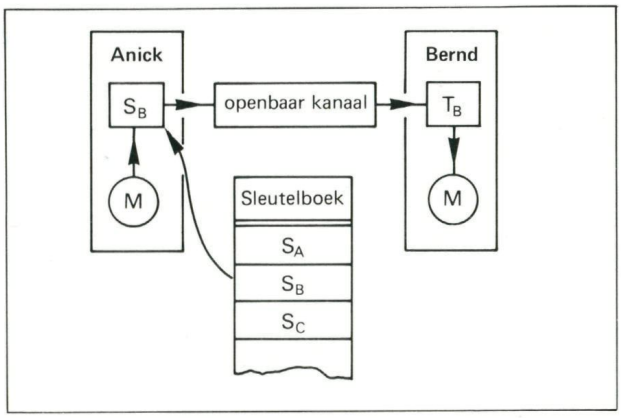
- Voer je S_G en T_G achter elkaar uit (de volgorde doet er niet toe), dan krijg je de oorspronkelijke boodschap (de klare tekst) terug.
- Het is praktisch ondoenlijk (zelfs met de krachtigste computers) om een bericht M te weten te komen als je alleen het vercijferde bericht $S_G(M)$ kent.

Die tweede eis is op het eerste gezicht niets bijzonders: bij alle cryptosystemen is het de bedoeling dat de klare tekst niet uit de vercijferde boodschap afgeleid kan worden. Nieuw is echter dat *alle* vercijfersleutels openbaar zijn. Iedereen kan elke S_G uitvoeren en het is ook precies bekend hoe elke S_G werkt. Maar S_G is een soort *eenrichtingsverkeer-functie:* de ene kant op – van M naar $S_G(M)$ – is gemakkelijk uit te voeren, maar de weg terug is, hoewel in theorie mogelijk, in de praktijk onuitvoerbaar omdat het eenvoudig veel te veel rekentijd vergt.
Tenzij . . .
Tenzij je over extra informatie beschikt waarmee je al dat werk kunt kortsluiten. En je begrijpt het waarschijnlijk al, die extra informatie zit verstopt in de privé sleutel T_G. Dat is een soort geheime deur waardoor je uit het doolhof $S_G(M)$ kunt ontsnappen zonder dat je alle gangen hoeft te proberen!
Bestaan er zulke eenrichtingsverkeer-functies met een geheime deur?
Dat is helemaal niet vanzelfsprekend. Ze moeten berusten op het praktisch onuitvoerbaar zijn van bepaalde opgaven. Maar wat vandaag onuitvoerbaar is, kan morgen met geavanceerdere technieken en grotere computers misschien wèl mogelijk zijn. Er zijn op dit moment systemen bekend die voorlopig nog veilig lijken. Ze berusten allemaal op technieken uit de hogere wiskunde. Verderop zullen we één zo'n systeem in grote lijnen schetsen. Maar laten we eerst uitleggen hoe Public Key Cryptosystemen in het algemeen werken, ervan uitgaande dat sleutelparen (S_G, T_G) met bovengenoemde twee eigenschappen bestaan.

Hoe werkt zo'n systeem?

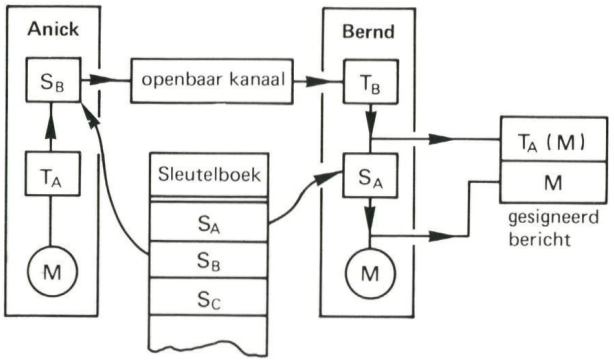
Stel Anick (A) wil een bericht M sturen naar Bernd (B) dat verder niemand mag weten. Ze zoekt dan in het sleutelboek Bernd's openbare steutel S_B op en typt M in op het toetsenbord van haar computer. Met haar computer berekent ze $S_B(M)$ en stuurt die over een openbaar kanaal naar Bernd.

Hoe stuurt Anick een bericht M naar Bernd?



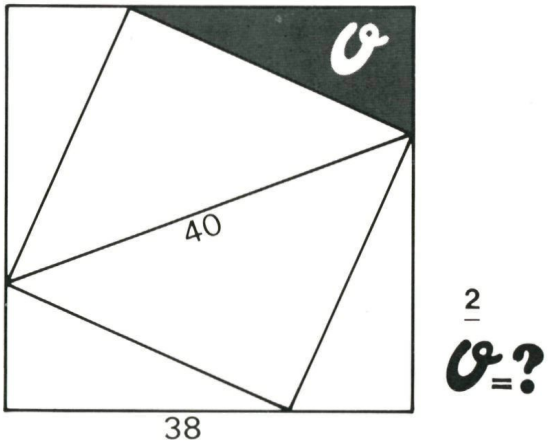
Een spion die dit vercijferde bericht $S_B(M)$ onderschept, kan er niets mee beginnen. Alleen Bernd kan met zijn privé sleutel T_B het bericht ontcijferen: $T_B(S_B(M)) = M$.
Maar Bernd is wantrouwend. Hij heeft het bericht M wel ontvangen, maar hoe weet hij zeker dat het van Anick komt? Iedereen kan immers boodschappen met S_B vercijferen. Anick kan aan dat bezwaar tegemoet komen als ze voortaan als volgt handelt.
Vóórdat ze haar klare tekst met de openbare sleutel S_B van Bernd vercijfert, moet ze er eerst haar eigen privé sleutel T_A op loslaten. Uit de klare tekst M maakt ze dus eerst $T_A(M)$. Daarna past ze er S_B op toe en stuurt Bernd de boodschap $S_B(T_A(M))$.

Hoe stuurt Anick een gesigneerd bericht M naar Bernd?



Ook geeft ze Bernd een (niet vercijferd) seintje dat er een geheim bericht van haar naar hem onderweg is. Na ontvangst berekent Bernd eerst met zijn privé sleutel T_B het *tussenbericht* $T_B(S_B(T_A(M))) = T_A(M)$. Daar wordt hij nog niet veel wijzer van. Maar met de openbare sleutel S_A van Anick (die hij uit het sleutelboek haalt) kan hij vervolgens de klare tekst $S_A(T_A(M)) = M$ berekenen. En wat meer is, hij weet nu ook zeker dat de boodschap van Anick afkomstig is. Want S_A toegepast op een boodschap die niet met Anick's privé sleutel T_A is vercijferd, zou alleen maar onzin opleveren. En Anick is de enige die T_A kent.

Als Bernd de tussenboodschap $T_A(M)$ samen met M bewaart, kan hij ook tegenover iedereen bewijzen dat Anick die boodschap heeft verstuurd, want iedereen kan controleren dat S_A toegepast op $T_A(M)$ inderdaad M oplevert. Zo is de combinatie van de twee boodschappen M en $T_A(M)$ dus gelijkwaardig met de boodschap M voorzien van Anick's *elektronische handtekening!*



$\frac{2}{\mathcal{O}=?}$

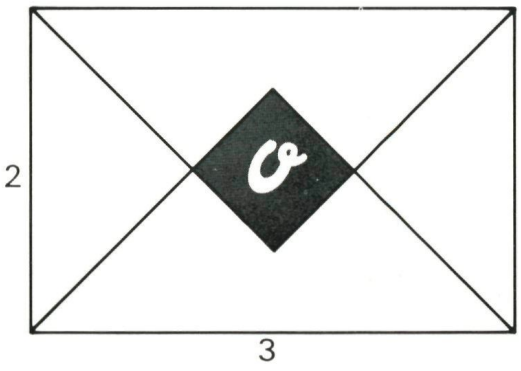
Het RSA-systeem

De eerste uitgewerkte Public Key Cryptosystemen zijn inmiddels al onveilig gebleken. De privé sleutels bleken met slimme wiskundige trucs opgespoord te kunnen worden. Maar in 1978 is door Rivest, Shamir en Adleman een systeem bedacht dat tot nu toe alle aanvallen heeft kunnen weerstaan, althans als we mogen afgaan op hetgeen er over is gepubliceerd. Hun systeem, dat naar hun initialen bekend staat als het RSA-systeem, zullen we hier uiteen zetten. We moeten daartoe eerst twee uitstapjes maken, één naar een supersnel algoritme voor machtsverheffen en een ander naar het zogenaamde modulair rekenen (ook wel klokrekenen genoemd).

Supersnel machtsverheffen

Op dit moment is het getal $2^{132049}-1$ het grootste bekende priemgetal. Kort na z'n ontdekking is het met al zijn 39751 cijfers o.a. afgedrukt in het Haarlems Dagblad. Dat nam een hele pagina in beslag! Hoe bepaal je zo'n getal in uitgeschreven vorm?

Die '−1' is natuurlijk geen probleem; het gaat om de macht van 2. Als je het op de voor de hand liggende manier doet – telkens met 2 vermenigvuldigen – kost het enorm veel tijd. Een computer die gemiddeld duizend vermenigvuldigingen per minuut uitvoert (bedenk dat de getallen op den duur duizenden cijfers tellen!), zou daar ruim twee uur over doen. Maar met het supersnelle algoritme zijn daar slechts 25 stappen voor nodig. Elke stap kost maar één vermenigvuldiging (plus aftrekken van 1, of delen door 2 van een klein even getal). Dat is, als je het handig programmeert, in hooguit een paar minuten gebeurd!



$\frac{3}{\mathcal{O}=?}$

Modulair rekenen

Modulair rekenen (of klokrekenen) kent iedereen. De uren van een klok reken je *modulo 12*, de minuten reken je *modulo 60*, de dagen van de week reken je *modulo 7*, en met de standen van een kilometerteller met 6 cijferposities reken je *modulo 1 miljoen.* Bij elke modulus m heb je alleen maar de getallen 0, 1, 2, ..., $m-1$ beschikbaar. Kom je bij m, dan begin je weer bij 0.

Je kunt optellen modulo m, vermenigvuldigen modulo m (want dat is herhaald optellen), en zelfs machtsverheffen modulo m (want dat is herhaald vermenigvuldigen).
Maak je bij modulair machtsverheffen gebruik van het supersnelle algoritme van hierboven, dan is er het bijkomende voordeel dat de getallen een vaste grootte (die van de modulus) niet te boven kunnen gaan, zodat in je algoritme de rekentijd per stap ook binnen de perken blijft.

Supersnelle algoritme

```
ALGORITME VOOR DE SUPERSNELLE BEREKENING VAN a^n
LEES a,        LEES n,
x:=a           y:=n,        z:=1
HERHAAL DIT BLOK ZOLANG
y≠0:
    HERHAAL DIT BLOK ZOLANG
    y EVEN IS:
        x:= x*x
        y:= y/2                (K)
    z:= x*z
    y:= y-1                    (V)
DRUK z AF
```

Commentaar *Nadat het algoritme is opgestart, wordt er telkens óf gekwadrateerd (K) óf vermenigvuldigd (V). Tevens wordt de waarde van y gehalveerd of met 1 verminderd. Op zeker moment bereik je $y = 0$, en dan stopt het algoritme.*
De snelheid van het algoritme berust op het feit dat y zo snel wordt afgebroken: er kunnen geen twee V-stappen achter elkaar voorkomen, dus elke twee stappen wordt y minstens gehalveerd.
De correctheid van het algoritme zit 'm in de relatie $a^n = (x^y) \times z$.
Die betrekking is in het begin geldig, en de geldigheid ervan wordt noch door (K), noch door (V) aangetast!

Aan het einde, als $y = 0$, heeft z dus de waarde a^n gekregen:
$a^n = (x^0) \times z = z$.

Voorbeeld *We berekenen 2^{30} en als variant ook 2^{30} modulo 55 (dan worden x en z dus telkens modulo 55 genomen). Aan het einde van elke regel vermelden we of een K-stap dan wel een V-stap is gebruikt.*

y	x	z	x mod 55	z mod 55	
30	2	1	2	1	
15	4	1	4	1	K
14	4	4	4	4	V
7	16	4	16	4	K
6	16	64	16	9	V
3	256	64	36	9	K
2	256	16384	36	49	V
1	65536	16384	31	49	K
0	65536	1073741824	31	34	V

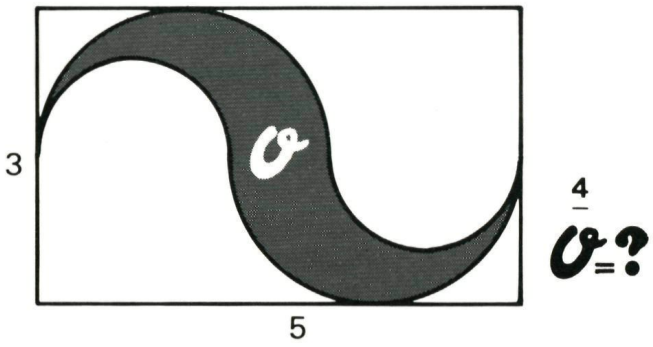
Dus $2^{30} = 1\,073\,741\,824$!
Ga eens na met welke 2-machten x en z uit deze tabel corresponderen. Je zult zien dat de slotwaarde $1\,073\,741\,824 = 2^{30}$ is opgebouwd als $2^2 \cdot 2^4 \cdot 2^8 \cdot 2^{16} = 2^{2+4+8+16}$.
De exponent 30 dus gesplitst als som van 2-machten. En dat gaat net zo bij andere exponenten n of grondtallen a.

Modulair machtsverheffen

Kies twee verschillende priemgetallen p en q, en bereken hun produkt m. Bijvoorbeeld $p = 5$ en $q = 11$, zodat geldt $m = 55$.
Begin nu met een willekeurig getal M kleiner dan m en bereken modulo m de machten
$M, M^2, M^3, \ldots$
Je zult zien dat dan op zeker moment het getal M terugkeert, waarna alles weer van voren af aan begint:
$M, M^2, M^3, \ldots, M^k, M^{k+1} = M, M^{k+2} = M^2, \ldots$ (modulo m).
In het bijzonder is dus
$M = M^{k+1} = M^{2k+1} = M^{3k+1} = \ldots$ (modulo m).
Het merkwaardige is nu – en dat volgt uit stellingen van Fermat (1601–1665) en Euler (1707–1783) – dat de periode k altijd een deler is van het getal $K = (p-1)(q-1)$, zodat voor alle M geldt
$M = M^{K+1} = M^{2K+1} = M^{3K+1} = \ldots$ (modulo m).
In ons geval, met $p = 5$, $q = 11$ en $m = 55$, is dus $K = 4 \cdot 10 = 40$, en je kunt met een computer gemakkelijk nagaan dat inderdaad voor elke M geldt dat $M = M^{41} = M^{81} = M^{121} = \ldots$ (modulo 55).

Vercijferen via machtsverheffen

We hebben nu alle voorbereidingen getroffen om het RSA-systeem uit te kunnen leggen. We zullen beschrijven hoe een sleutelpaar (S, T) van een gebruiker van het systeem werkt. In een apart kader hebben we het in een paar woorden samengevat.



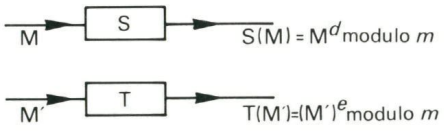
Elke gebruiker begint met twee grote priemgetallen p en q, elk van ongeveer honderd cijfers. Met geavanceerde technieken is het tegenwoordig mogelijk om zulke priemgetallen zeer snel te fabriceren. Het produkt $m = p \cdot q$ is dan een getal van ongeveer 200 cijfers. Na het kiezen van p en q en het berekenen van m, bepaalt de gebruiker het getal $K = (p-1)(q-1)$, alsmede een groot getal d, kleiner dan K, dat met K geen delers gemeen heeft. Daarmee zijn de voorbereidingen voor de openbare sleutel S getroffen.
Het vercijferen van een klare tekst of bericht M (dat gegeven moet zijn in de vorm van een getal kleiner dan m; berichten die te lang zijn splits je in stukken) gaat als volgt:
$S(M) = M^d$ (modulo m).
Om S uit te kunnen voeren, moet je dus m en d kennen. Die twee getallen worden dan ook openbaar gemaakt. Maar let op, de oorspronkelijke priemgetallen p en q moeten geheim blijven! Daarmee zullen we zo dadelijk de privé sleutel T construeren. We weten dat je met het supersnelle algoritme heel snel S (M) uit M kunt berekenen, zelfs als d, m en M honderd of meer cijfers tellen.

Nu de privé sleutel.
Het ontcijferen gebeurt door S (M) ook weer tot een zekere macht te verheffen:
$T(S\,M)) = (S\,M))^e = (M^d)^e = M^{d \cdot e}$ (modulo m).
Daarbij is het getal e zó gekozen dat het produkt $d \cdot e$ van de vorm $j \cdot K + 1$ is voor zekere j. Dan is namelijk $M^{de} = M^{jK+1} = M$ (modulo m) op grond van wat we in het voorgaande stuk hebben afgeleid.
Dat er inderdaad zo'n getal bestaat, volgt uit een stelling van Euclides (ca. 300 v. Chr.), die ook een snel algoritme beschreef om een getal e te berekenen als je d en K kent. Voorwaarde is wel dat d en K geen gemeenschappelijke delers mogen hebben, maar dat hebben we hierboven geëist.
De privé sleutel T komt dus neer op machtsverheffen modulo m met exponent e. En die exponent e konden we bepalen omdat we het getal $K = (p-1)(q-1)$ kennen, en K kennen we omdat we de ontbinding $m = p \cdot q$ van m kennen. De veiligheid van onze privé sleutel berust dus op de praktische onmogelijkheid om getallen van zo'n tweehonderd cijfers in factoren te ontbinden!

De sleutels bij het RSA-systeem

Iedere gebruiker verschaft zich twee priemgetallen p en q die elk uit ongeveer honderd cijfers bestaan. Vervolgens bepaalt hij hun produkt $m = p \cdot q$ en het getal $K = (p-1)(q-1)$.
Dan kiest hij een groot getal d kleiner dan K, dat met K geen delers gemeen heeft, en bepaalt met het algoritme van Euclides een getal e zo, dat $d \cdot e$ van de vorm $jK + 1$ is voor zekere j.
Alleen de getallen m en d maakt hij bekend. De andere getallen p, q, K en e houdt hij geheim.

Z'n openbare sleutel S en z'n privé sleutel T zijn nu als volgt gedefiniëerd:



(De getallen M en M' moeten kleiner zijn dan m.)

Een voorbeeld met kleine getallen
$p = 5, q = 11, m = 55, K = 4 \cdot 10 = 40$
Kies bijvoorbeeld $d = 33$ dan wordt e gelijk aan 17, want $17 \cdot 33 = 561 = 14 \cdot 40 + 1$.
Neem nu een boodschap gecodeerd als bijvoorbeeld $M = 20$. Dan is $S(M) = 20^{33}$ (modulo 55) $= 25$ en $T(S(M)) = 25^{17}$ (modulo 55) $= 20$.
Berekeningen (alles modulo 55):

$S(M) = 20^{33}$

y	x	z
33	20	1
32	20	20
16	15	20
8	5	20
4	25	20
2	20	20
1	15	20
0	15	25

dus $S(M) = 25$

$T(S(M)) = 25^{17}$

y	x	z
17	25	1
16	25	25
8	20	25
4	15	25
2	5	25
1	25	25
0	25	20

dus $T(S(M)) = 20 = M$

Hoe veilig is het RSA-systeem?

Je zult er misschien vreemd van opkijken dat zo iets simpels als het ontbinden van een getal in factoren moeilijk zou kunnen zijn. Het is ook helemaal niet moeilijk. Je begint gewoon maar de rij van de priemgetallen af te lopen en te kijken of ze het getal delen. Maar probeer je eens te realiseren hoeveel testen je zou moeten uitvoeren bij een getal van tweehonderd cijfers. Zelfs al zou je weten dat er een factor van honderd cijfers in zou zitten, dan weet je nog niet hoe je die zou moeten vinden. Heb je je wel eens gerealiseerd hoeveel getallen van honderd cijfers er zijn?
Ontbinden in factoren blijkt in de praktijk zelfs met de meest verfijnde wiskundige technieken een ontzettend bewerkelijke opgave te zijn. Op dit moment kan men getallen van zo'n zeventig cijfers de baas, maar tweehonderd cijfers ligt nog ver buiten het bereik. Voor hoe lang nog?
Je zou ook op andere manieren kunnen proberen om de klare tekst M uit S(M) af te leiden. Bijvoorbeeld door domweg alle machten van S(M) af te lopen (modulo m). Eens zal er dan een zinnige boodschap verschijnen, want $M = (S(M))^e$. Maar het zal duidelijk zijn dat als e groot is, ook deze methode praktisch ondoenlijk is.
Tot nu toe heeft het RSA-systeem alle kritiek kunnen doorstaan. Alle pogingen om het systeem te kraken, hebben schipbreuk geleden. Men heeft er wel voor gezorgd dat er aan de keuze van p en q nog enige extra eisen worden opgelegd om de veiligheid nog verder te garanderen, maar het zou te ver voeren daar op deze plaats op in te gaan.
Maar zoals altijd in de cryptografie, iemand die het systeem kan breken, heeft er vaak alle belang bij om dat geheim te houden.
Dus wie weet . . .!?

Een reuzenontbinding

Getallen vermenigvuldigen hoor je te kunnen: 7 X 11 X 13 (vermenigvuldigd) = 1001.
Het omgekeerde, het ontbinden in factoren, is eigenlijk veel interessanter:
1001 (ontbonden) = 7 X 11 X 13
Dit splitsen van een getal blijkt veel moeilijker dan het uitcijferen van een vermenigvuldiging. Zó moeilijk dat alleen van kleine getallen (nou ja) bekend is of, en zo ja hoe, ze in factoren ontbonden kunnen worden. Als van een wat groter getal de ontbinding gevonden wordt, komt dat soms zelfs in de krant. Zoals in 1984 het geval was voor het getal hieronder. Probeer maar in hoeverre je kunt controleren of het wel klopt (eindcijfers, begincijfers, aantal cijfers, enz.). De factoren zijn alle vijf priemgetallen, er kan dus niet verder worden gesplitst.

$$2^{251} - 1$$

=

3 618 502 767 861 666 131 107 987 593 282 521 497 120 415 687 021 801 268 626 233 050 500 247 285 301 247

=

503

X

54 217

X

178 230 287 214 063 289 511

X

61 676 882 198 695 257 501 367

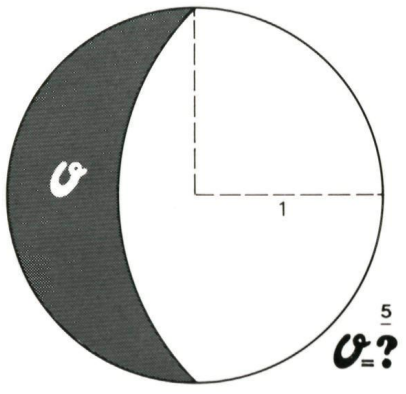
X

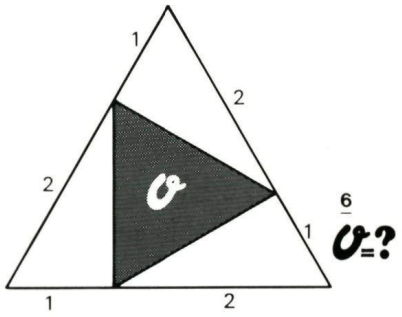
12 070 396 178 249 893 039 969 681

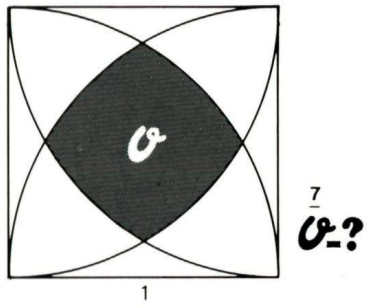
Geheimen in gevaar?

De twee 'kleine' factoren waren al langer bekend, maar er bleef een getal van 69 cijfers over waarvan tot voor kort gedacht werd dat z'n ontbinding wel nooit gevonden zou worden. Dit omdat het rekenwerk, zelfs voor de grootste computers, veel en veel te groot leek.
De moeilijkheid van het ontbinden van grote getallen vormt de basis van het RSA-systeem (zie het artikel 'Geheimschrift IV' in dit nummer), waarmee geheime berichten veilig verstuurd kunnen worden. Het werkt met getallen van zo'n tweehonderd cijfers en op dit moment zijn die nog praktisch onontbindbaar. Maar de ontwikkelingen verlopen stormachtig: in 1975 was het nog ondoenlijk om getallen van 40 cijfers te ontbinden. Hierboven zie je dat getallen van zo'n 70 cijfers al geen probleem meer vormen. Ook van vorig jaar dateert de ontbinding van 11111... 11111 (71 enen) in twee priemfactoren van respectievelijk 30 en 41 cijfers.

En als je niet gelooft dat ontbinden in de praktijk echt heel moeilijk is, moet je je krachten (of die van je computer?) maar eens beproeven op de getallen
111 . . . 11 (17 enen)
111 . . . 111 (18 enen)
111 . . . 1111 (19 enen)
Eén van deze drie getallen is veel gemakkelijker te ontbinden dan de andere. Zie je welke?







Nederlandse Wiskunde Olympiade

Oplossingen Tweede Ronde Nederlandse Wiskunde Olympiade 1984

1 Laten A_1 en A_2 de middelpunten zijn van de cirkels C_1 en C_2, en stel dat de lijn PA_1A_2 de cirkel C_2 nogmaals snijdt in T. Omdat A_1RSP een vierkant is, deelt PR hoek TPS middendoor. We zijn klaar als we kunnen bewijzen dat $< TPM = < SPN$. Omdat $< TMP = \frac{\pi}{2}$ (want TP is een middellijn van C_2), geldt $< TPM = \frac{\pi}{2} - < MTP = \frac{\pi}{2} - < NPT = < SPN$ (merk op dat $TMNP$ een gelijkbenig trapezium is!).

Als PN hoek RPS middendoor deelt, is $< NPA_2 = \frac{3\pi}{8}$.

$A_2P = A_2N$, dus $< NPA_2 = < PNA_2$ en daarom is $< PA_2N = \pi - 2 \cdot \frac{3\pi}{8} = \frac{\pi}{4}$. Ook $< A_2PR = \frac{\pi}{4}$, en omdat $RN \| A_2P$ volgt hieruit $PR = A_2N = r_2$.

A_1RSP is een vierkant, dus $r_1 : r_2 = A_1R : PR = 1 : \sqrt{2}$.

2 Een notatie als (124) betekent dat de schakelaars S_1, S_2 en S_4 gesloten zijn (en de andere open). In de volgende, elkaar uitsluitende situaties brandt het lampje

(12345)	(124)	(123)
(1234)	(125)	(345)
(1235)	(145)	(12)
(1245)	(245)	(45)
(1345)	(135)	
(2345)	(234)	

In alle andere gevallen brandt het lampje niet.

Als 3 in het rijtje voorkomt, is de kans $\frac{2}{3}(\frac{1}{2})^4$, anders $\frac{1}{3}(\frac{1}{2})^4$.

Optellen geeft in totaal een kans van $\frac{25}{48}$ dat het lampje brandt.

3 Uit de definitie van a_n volgt $a_{n+1} = \frac{3n+1}{3n+2} \cdot a_n$.

De linker ongelijkheid is equivalent met $a_n^2(3n+1) \geqslant 1$. Noem het linkerlid hiervan b_n, dan is $b_{n+1} = a_{n+1}^2 \cdot$

$$(3n+4) = a_n^2 \cdot \frac{(3n+1)^2}{(3n+2)^2} \cdot (3n+4) = b_n \cdot \frac{(3n+1)(3n+4)}{(3n+2)^2} =$$

$$= b_n \frac{9n^2+15n+4}{9n^2+12n+4} > b_n. \text{ (mits } n \geqslant 1).$$

De rij $\{b_n\}$ is dus *stijgend*, en aangezien $b_1 = 1$, geldt voor alle n $b_n \geqslant 1$.

Het bewijs van de rechter ongelijkheid gaat net zo. Stel nu $c_n = a_n^3(3n+1)$. Te bewijzen is dat $c_n < 1$ voor alle n. Maar $\{c_n\}$ is een *dalende* rij, want $c_{n+1} = c_n \cdot \frac{(3n+1)^2(3n+4)}{(3n+2)^3} =$

$$c_n \cdot \frac{27n^3+54n^2+27n+4}{27n^3+54n^2+36n+8} < c_n.$$

Omdat $c_1 = \frac{1}{2}$ volgt hieruit $c_n \leqslant \frac{1}{2} < 1$ voor alle n, hetgeen te bewijzen was.

4 Haakjes plaatsen geeft uiteindelijk een uitdrukking van de vorm $A:B$, waarin A en B uitdrukkingen tussen haakjes zijn (of een losse factor). Voeg je een nieuwe factor n toe:

$A : B : n$

dan kun je n door haakjes naar keuze in de teller of in de noemer krijgen:

$$A : (B : n) = \frac{A \cdot n}{B} \quad (1)$$

$$(A : B) : n = \frac{A}{B \cdot n} \quad (2)$$

Na uitwerken van de uitdrukkingen A en B ontstaat een breuk met

- in geval (1) de factor n in de teller,
- in geval (2) de factor n in de noemer.

Verder blijft de factor 1 altijd in de teller, en de factor 2 altijd in de noemer.

Hieruit blijkt dat je als getalwaarde elke breuk kunt krijgen met factor 1 in de teller, factor 2 in de noemer, en de factoren 3 t.e.m. 8 willekeurig verdeeld over teller en noemer. De *grootste* getalwaarde is dus

$$\frac{1 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8}{2} = 1 : ((((((2:3):4):5):6):7):8) =$$

$$= 10080$$

en de kleinste is

$$\frac{1}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8} = ((((((1:2):3):4):5):6):7):8 =$$

$$= \frac{1}{40320}.$$

Er zijn $2^6 = 64$ mogelijkheden om 3 t.e.m. 8 over teller en noemer te verdelen, maar ..... $3 \cdot 8 = 4 \cdot 6$, en dat betekent dat sommige verdelingen *dezelfde* getalwaarde opleveren:

$$\frac{1 \cdot 5 \cdot 7 \cdot 3 \cdot 8}{2 \cdot 4 \cdot 6} = \frac{1 \cdot 5 \cdot 7 \cdot 4 \cdot 6}{2 \cdot 3 \cdot 8}, \quad \frac{1 \cdot 5 \cdot 3 \cdot 8}{2 \cdot 7 \cdot 4 \cdot 6} = \frac{1 \cdot 5 \cdot 4 \cdot 6}{2 \cdot 7 \cdot 3 \cdot 8},$$

$$\frac{1 \cdot 7 \cdot 3 \cdot 8}{2 \cdot 5 \cdot 4 \cdot 6} = \frac{1 \cdot 7 \cdot 4 \cdot 6}{2 \cdot 5 \cdot 3 \cdot 8}, \quad \frac{1 \cdot 3 \cdot 8}{2 \cdot 5 \cdot 7 \cdot 4 \cdot 6} = \frac{1 \cdot 4 \cdot 6}{2 \cdot 5 \cdot 7 \cdot 3 \cdot 8}.$$

Er zijn daarom slechts $64 - 4 = 60$ verschillende getalwaarden mogelijk.

Pythagoras Olympiade

Nieuwe opgaven (Oplossingen inzenden vóór 30 mei 1985 aan *Pythagoras Olympiade, Cornelis Krusemanstraat 60II, 1075 NS Amsterdam (NL).*
Wedstrijdvoorwaarden en prijzen zijn vermeld op pagina 8 van deze jaargang.)

PO 79
Gegeven is een scherphoekige driehoek met zijden a_1, a_2 en a_3 en omgeschreven cirkel C. Voor $i = 1, 2, 3$,is C_i het spiegelbeeld van C in zijde a_i.
Bewijs dat de cirkels C_1, C_2 en C_3 door één punt gaan.

PO 80
a Toon aan dat het getal $k = 1985! - 1984!$ op precies 1985 nullen eindigt als je het in het tweetallig stelsel uitschrijft.
b Hoe kun je in het algemeen aan de schrijfwijze van een getal n in het tweetallig stelsel zien of het getal $k(n) = n! - (n - 1)$ in dat stelsel op precies n nullen eindigt?

PO 81
Aan het begin van een feestje met 9 deelnemers hebben sommige mensen elkaar ter begroeting gezoend. Bewijs dat minstens één van de volgende twee beweringen waar is:
1 Er zijn minstens drie mensen die elkaar geen van alle gezoend hebben.
2 Er zijn minstens vier mensen die elkaar allemaal gezoend hebben.
(Hèt zoenen was steeds wederzijds: ieder die een zoen kreeg, gaf er ook een terug.)

Opmerking: PO 80 is verzonnen door de oud-deelnemers aan de Pythagoras Olympiade Harold de Boer uit Nijeveen en Bart de Smit uit Amsterdam op de terugreis uit Praag na hun deelname aan de Internationale Wiskunde Olympiade 1984.

Oplossingen en prijswinnaars van de opgaven PO 67–69

PO 67
Voor een zeker natuurlijk getal n is $10^n + 1$ een priemgetal groter dan 2.
Bewijs dat n van de vorm $n = 2^k$ is voor zeker natuurlijk getal k.

Oplossing van *Jan de Boer*, 6 vwo, RSG Magister Alvinus, Sneek:
Voor alle oneven q is $a^{pq} + b^{pq} = (a^p + b^p)(a^{p(q-1)} - b^p a^{p(q-2)} + b^{2p} a^{p(q-3)} - \ldots\ldots - b^{p(q-2)} a^p + b^{p(q-1)})$. Als n dus een oneven factor, zeg r, bevat, dan is $10^n + 1 = 10^n + 1^n$ deelbaar door $10^{n/r} + 1^{n/r}$, en dus geen priemgetal. Dus n mag geen oneven factoren bevatten, en daarom is n van de vorm $n = 2^k$.

Er waren 21 inzendingen, waarvan 14 correct. Prijswinnaars: *Wiebe Kees Goodijk*, 6 g Christelijk Gymnasium Leeuwarden, en *Willem Brussaard*, 5 havo, Van Lodestein HSG, Amersfoort.

PO 68
Voor elke niet-lege deelverzameling $D = i_1, \ldots, i_k$ van de verzameling 1, 2, . . ., 1984 definiëren we het getal $p(D)$ door $p(D) = \dfrac{1}{i_1 \cdot i_2 \cdot \ldots \cdot i_k}$.

Bewijs dat de som van alle getallen $p(D)$ 1984 is.

Eerste oplossing van Frank Robijn, 6 g, RSG Koning Willem II, Tilburg:
Noem $V(n) = 1, 2, \ldots, n$, en laat $s(n)$ de som zijn van alle $p(D)$ behorende bij niet-lege deelverzamelingen van $V(n)$. De collectie van alle niet -lege deelverzamelingen van $V(n + 1)$ kunnen we splitsen in
- alle niet-lege deelverzamelingen van $V(n)$; de som van hun getallen $p(D)$ is $s(n)$,
- diezelfde verzamelingen uitgebreid met het element $(n + 1)$. De bijbehorende som is dan $s(n)/(n + 1)$,
- de deelverzameling $n + 1$, met als sombijdrage $\dfrac{1}{n+1}$.

Er geldt dus $s(n + 1) = s(n) + \dfrac{1}{n+1}(s(n) + 1)$.

Omdat $s(1) = 1$ volgt hieruit $s(2) = 2$, dan $s(3) = 3$, enz., dus $s(1984) = 1984$.

Tweede oplossing van *Jan de Boer*, 6 vwo, RSG Magister Alinus, Sneek:
Als je het getal $N = (1 + \frac{1}{1})(1 + \frac{1}{2})(1 + \frac{1}{3}) \ldots . (1 = \frac{1}{1984})$
uitschrijft, komt er eerst het getal 1, en daarna alle getallen $p(D)$, elk precies één maal. De som van alle getallen $p(D)$ is dus
$N - 1 = (1 + \frac{1}{1})(1 + \frac{1}{2}) \ldots (1 + \frac{1}{1984}) - 1 = \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{3} \cdot \ldots \cdot \frac{1985}{1984} - 1 = 1985 - 1 =$
$= 1984.$

Er waren 18 inzendingen, waarvan 14 correct. Prijswinnaars: *Frank Robijn*, en *Harry Boomsma*, 6 vwo, Stedelijk Gymnasium, Leeuwarden.

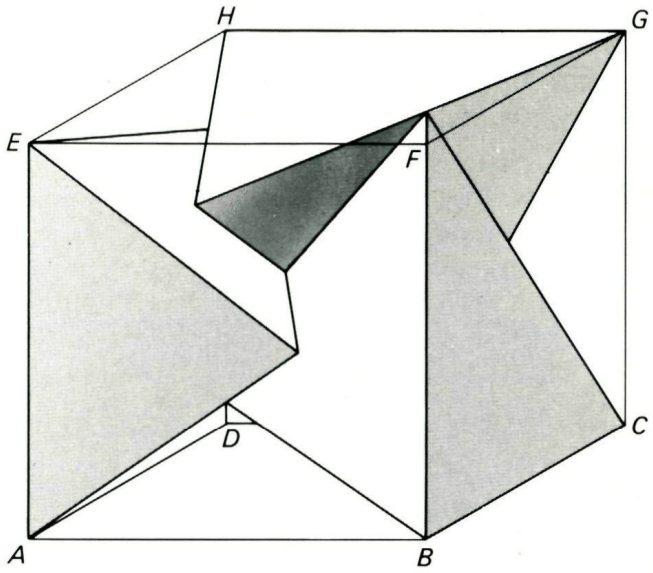
PO 69

Toon aan dat je in een kubusvormige holle doos met inwendige ribbelengte 1, drie massieve regelmatig viervlakken met ribbelengte 1 kunt opbergen. (Geef bijvoorbeeld een nette tekening met een duidelijke toelichting.)

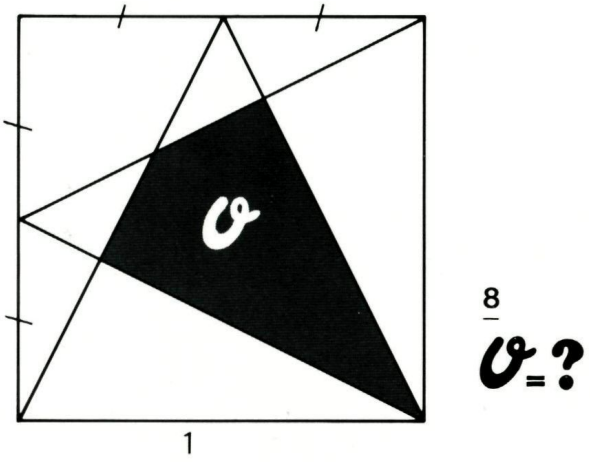
Oplossing: Elk viervlak moet zo geplaatst worden dat één ribbe ervan samenvalt met een ribbe van de kubus, en dat het midden van de tegenoverliggende ribbe van het viervlak precies samenvalt met het centrum van de kubus. Je kunt uitrekenen (en de goede oplossers hebben dat gedaan) dat de afmetingen van het viervlak zó zijn, dat dit inderdaad precies kan. De drie viervlakken leg je nu langs drie kruisende ribben van de kubus (bijv. in de kubus *ABCD.EFGH* de ribben *AB*, *FG* en *DH*). De drie viervlakken raken elkaar dan precies in het centrum van de kubus, en alles past precies!

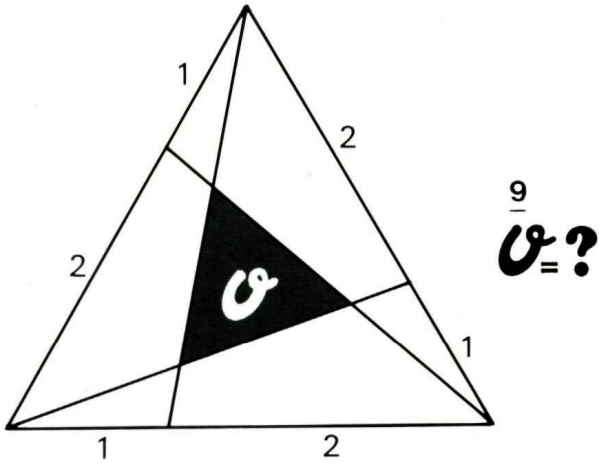
We kregen 20 inzendingen, waarvan 15 correct. Een aantal heel mooie tekeningen willen we apart noemen: die van *Jan de Boer, Harold de Boer*, 6 vwo, CSG Dingstede, Meppel, *Wiebe Kees Goodijk, Wim v.d. Graaf*, 5 g, Eindhovens Protestants Lyceum, *Caroline Hummels*, 5 vwo, Pius X College, Almelo, *Elke Laarhuis*, 5 atheneum., OSG Bataafse Kamp, Hengelo (Ov), *Menke Ubbens*, 6 vwo, RSG Magister Alvinus, Sneek.

Prijswinnaars: *Wim v.d. Graaf*, en *Floor van Lamoen*, 6 vwo, stedelijk Gymnasium, Leeuwarden.



Deze tekening zond Caroline Hummels, 5 vwo, Pius-X-College te Almelo in bij haar oplossing van PO 69.





Oplossingen O-tjes

1 $\pi/2-1$
2 161
3 1/2
4 $(5\pi)/4$
5 1
6 $(3\sqrt{3})/4$ (één-derde van het totaal!)
7 $1+\pi/3-\sqrt{3}$
8 4/15
9 $(9\sqrt{3})/28$ (één-zevende van het totaal!)

Help de wolf

Wolf en schapen is een bekend spelletje op het dambord. De wolf moet door de linie van de schapen zien te breken. De schapen mogen alleen vooruit, maar de wolf mag vooruit èn achteruit.
Als de schapen verstandig spelen, heeft de wolf geen schijn van kans. Daarom verveelt het snel. Je kunt de wolf echter wat helpen. Als je hem bijvoorbeeld in het begin zijn uitgangspositie laat kiezen, kan hij het de schapen heel wat lastiger maken.
Nog beter is het als hij één keer in het hele spel een beurt mag overslaan. Zo wint hij in de hieronder afgebeelde positie (met de schapen aan zet), als hij één keer mag 'passen'.
Zouden de schapen bij verstandig spel ook nu nog altijd kunnen winnen?
Als de wolf in totaal *tweemaal* mag passen, dan kan hij volgens ons in elk geval altijd door de schaapslinie heenbreken.
Probeer het maar!