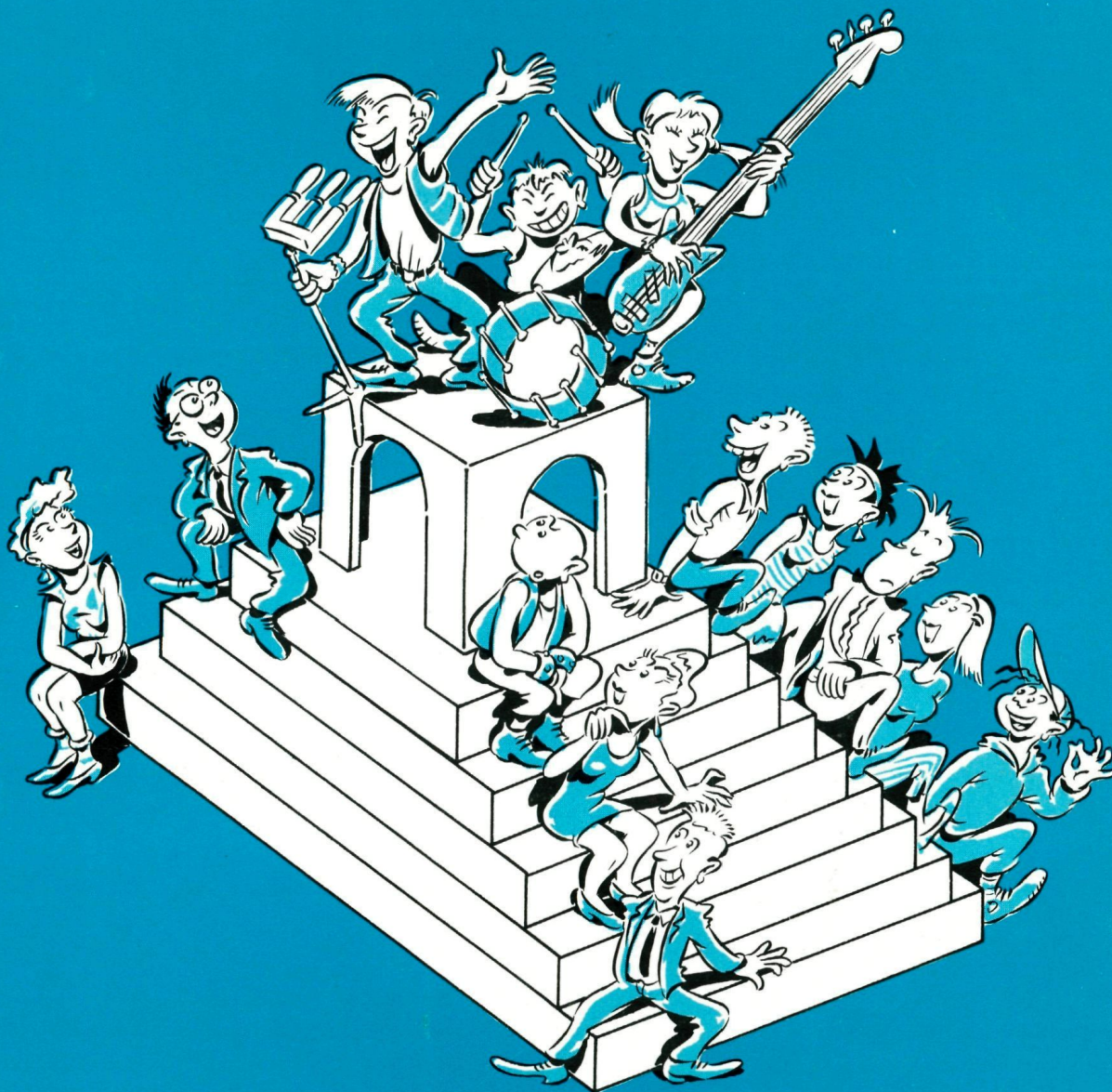
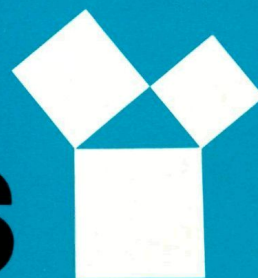




Verschijnt vier keer per jaar

Wiskundetijdschrift voor jongeren

Pythagoras



1 Jaargang 24 oktober 1984

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, Egelandierstraat 107^{II}
1015 PZ Amsterdam

Illustraties Evert Geradts, Piet Agoras

Foto's

Presse- und Informationsamt der Bundesregierung,
Bonn: blz. 3
Niedersächsische Landesbibliothek, Hannover: blz. 5
B.B.C. Hulton Picture Library, London: blz. 15
Battus, Opperlandse taal- en letterkunde,
uitg. Querido. 1981: blz. 17.

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 8081-30.
Abonnees wordt dringend verzocht met betalen te wachten tot een acceptgirokaart wordt gezonden.

Het geheel of gedeeltelijk overnemen van de inhoud zonder voorafgaande schriftelijke toestemming van de redactie is niet toegestaan.

Inhoud

Gottfried Wilhelm Leibniz (1646–1716)	3
<i>Jan van Maanen</i>	
Correspondentie (De 5 vijven)	6
Eén metertje meer...	7
<i>Jan van de Craats / Luc Kuijk / Hans de Rijk</i>	
Pythagoras Olympiade (spelregels en uitslag)	8
<i>Jan van de Craats</i>	
Geheimschrift I	9
<i>Klaas Lakeman</i>	
Palindromen	17
<i>Klaas Lakeman / Leo Wiegerink</i>	
Leibniz' nieuwe methode	20
<i>Jan van Maanen</i>	
Pythagoras Olympiade	22
<i>Jan van de Craats</i>	
Teveel of tekort?	24
<i>Leo Wiegerink</i>	

Bij de voorplaat Waarschijnlijk zijn de toeschouwers zó geboeid door de muziek dat ze het onmogelijke van hun situatie niet opmerken. De trap waarop ze zitten is namelijk een voorbeeld van een **onmogelijke figuur**, een tekening van een (ruimtelijk) voorwerp, dat in werkelijkheid niet kan bestaan.

In het verleden zijn er wel meer van dit soort figuren in Pythagoras opgenomen. Daarbij is gebleken dat er veel belangstelling voor bestaat. Daarom is er onlangs een werkgroep opgericht, die zich speciaal met onmogelijke figuren bezig gaat houden. Heb je daar ook belangstelling voor, dan kun je je opgeven bij:

Bruno Ernst, Stationsstraat 114, 3511 EJ Utrecht.



— Gottfried Wilhelm Leibniz (1646 – 1716) —

1984 is een bijzonder getal (lees maar verder) en een bijzonder jaar. Want zoals elk jaar kent ook 1984 weer talrijke herdenkingen. Een mijlpaal in de wiskunde werd bereikt in 1684. In dat jaar presenteerde Leibniz namelijk in de 'Acta Eruditorum' (Mededelingen van geleerden), een sinds 1682 in Leipzig verschijnend wetenschappelijk tijdschrift, de ontdekking van de differentiaalrekening, in zijn eigen woorden de 'nieuwe methode'. (In het artikel 'Leibniz' nieuwe methode' op pagina 20 wordt uitvoerig ingegaan op de inhoud van die publicatie.)

Die ontdekking betekende een grote stap (zo niet sprong) voorwaarts in de ontwikkeling van de wiskunde. Ze wordt daarom in 1984 op allerlei manieren herdacht: met een internationaal congres dat in augustus in Noordwijkerhout plaatsvond, met een serie artikelen in een gedenkboek, en... bij deze in Pythagoras.

Leven

Leibniz werd in Leipzig geboren, twee jaar voor het einde van de Dertigjarige Oorlog, die Duitsland zwaar getroffen heeft: één derde van de bevolking kwam om. Al vroeg verloor hij zijn ouders: in 1652 zijn vader die notaris en hoogleraar was, en in 1664 zijn moeder. Vanaf zijn vijftiende studeerde hij theologie, filosofie en rechten, en later ook wiskunde. Toen hij na vijf jaar studie wilde promoveren in de rechten, werd hem dat vanwege zijn jeugdige leeftijd in Leipzig geweigerd. Daarom verliet hij zijn vaderstad, en promoveerde in Altdorf. Daar bood men hem een professoraat in de rechten aan. Maar dat sloeg hij af, en koos voor de diplomatieke dienst.

Problemen met het buitenland waren er te over. Er dreigde gevaar van de Turken, en vooral van de Fransen onder leiding van Lodewijk XIV, de Zonnekoning. In dienst van de keurvorst van Mainz werkte Leibniz een plan uit om de aandacht van de opdringende Fransen in een andere richting te buigen. Hij wilde ze namelijk wijzen op het belang van een 'heilige oorlog' tegen Egypte, dat vanzelfsprekend gekerstend moest worden, en bovendien veel rijkdommen bezat.

In 1672 werd hij naar Parijs gestuurd om daar zijn plan voor te leggen. Hij ging vergeefs, want toen hij daar aankwam, was de oorlog tegen de Duitse staten reeds uitgebroken.

Kort daarop, in 1673, overleed de keurvorst van Mainz, en trad Leibniz als bibliothecaris en juridisch adviseur in dienst van de hertog van Hannover. Ondanks diens aandringen wist Leibniz zijn vertrek naar Hannover tot 1676 uit te stellen.

Tot zijn dood bleef hij, afgezien van talrijke reizen, in Hannover werkzaam. De laatste jaren van zijn leven vielen hem echter zwaar. Hij was in ongenade gevallen bij het hof, en leed een eenzaam bestaan. Na een jarenlange ziekte overleed hij in 1716.

Leibniz is het grote voorbeeld van iemand die op vele terreinen van de wetenschap thuis was. Niet alleen in de wiskunde, maar ook in de filosofie, de geschiedschrijving en de rechtswetenschap heeft hij baanbrekend werk verricht. En dat deed hij dan naast alle dagelijkse besommeringen aan het hof (boeken kopen, de mijnbouw in de Harz organiseren, waarvoor hij windmolens liet bouwen, enz.)

Aanzet tot de nieuwe methode

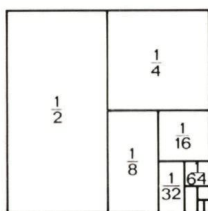
Voor de wiskundige ontwikkeling van Leibniz waren de jaren in Parijs van doorslaggevende betekenis. Parijs was een cultureel centrum bij uitstek. Er waren wetenschappelijke bijeenkomsten, en er was geld om geleerden van formaat aan te trekken. Hun onbetwiste leider was de Nederlandse wiskundige, astronoom en natuurkundige Christiaan Huygens (1629–1695), die van 1663 tot 1681 grotendeels in Parijs werkte.

Onder leiding van Huygens zette Leibniz zich weer aan de wiskunde. Hij werd onder andere zeer geboeid door oneindige getallenrijen.

Een voorbeeld van zo'n rij is:

$$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \dots$$

De som van de eerste n getallen (of termen) uit deze rij is $1 - (\frac{1}{2})^n$. En omdat je $(\frac{1}{2})^n$ net zo dicht bij 0 kunt brengen als je wilt door n maar groot genoeg te maken, kun je de som net zo dicht bij 1 krijgen als je maar wilt (zie onderstaande figuur). We zeggen daarom dat de som (van alle getallen van) die rij 1 is.



In Leibniz' tijd was ook bekend dat niet elke rij waarvan de getallen willekeurig dicht bij 0 komen, een eindige som heeft. Zo had men ontdekt dat de som van de rij:

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}, \frac{1}{9}, \frac{1}{10}, \dots, \frac{1}{15}, \frac{1}{16}, \frac{1}{17}, \dots, \frac{1}{32}$$

oneindig is. De som van de getallen boven één haak is namelijk steeds minstens gelijk aan $\frac{1}{2}$. En door nu maar ver genoeg te gaan, kun je de som van de eerste n getallen net zo groot krijgen als je wilt.

Het was dus een hele kunst om na te gaan of een rij een eindige som heeft, en als dat zo is, om die som te berekenen. Juist die ervaring met het optellen van getallen van een rij zou Leibniz later goed van pas komen bij het ontwikkelen van zijn nieuwe methode.

4 Pythagoras

Vergelijkingen en grafieken

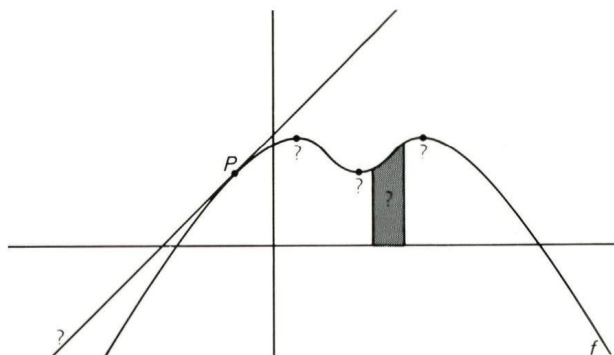
Het verband tussen vergelijkingen in x en y (zoals bijvoorbeeld $y = x^2$) en krommen in een assenstelsel (in dit voorbeeld een parabool) is voor ons vanzelfsprekend. Dat is echter lang niet altijd zo geweest. Vergelijkingen hoorden thuis in de algebra, krommen in de meetkunde. Niemand zag in dat die twee gebieden iets met elkaar te maken konden hebben.

De Franse filosoof René Descartes (1596–1650) bracht daar verandering in. In 1637 schreef hij een boek om zijn nieuwe filosofie uiteen te zetten, en dat boek had een aanhangsel getiteld 'La Géométrie'. Daarin gebruikte Descartes als eerste in de wiskunde assen en coördinaten, waarmee hij vervolgens het verband liet zien tussen krommen en vergelijkingen. Na deze publicatie kon men dan ook krommen (we zeggen nu liever grafieken) gaan onderzoeken door naar hun vergelijkingen te kijken.

In de herfst van 1675 ging ook Leibniz zich met dat soort onderzoekingen bezighouden. Op advies van Huygens las hij daar een aantal boeken over. Hij merkte dat de onderstaande drie problemen daarin telkens terugkwamen (zie ook onderstaande figuur).

Stel dat van een kromme f het functievoorschrift bekend is,

- kun je dan de oppervlakte tussen een gegeven deel van de kromme en de x -as uitrekenen (*het probleem van de quadratuur*)?
- kun je dan in een gegeven punt van de kromme de vergelijking van de raaklijn bepalen (*het tangenten-probleem*)?
- kun je dan bepalen waar de hoogste en de laagste punten van de kromme liggen (*het probleem van de maxima en de minima*)?



Voor sommige krommen had men tussen 1637 en 1675 deze drie vragen kunnen beantwoorden. Maar een voor alle soorten krommen toepasbare oplossingsmethode was er nog niet. Uitgaande van zijn ervaring met getallenrijen wist Leibniz nu zo'n algemene methode te ontwikkelen. Die publiceerde hij in 1684 onder de (hier iets ingekorte) titel: *Een nieuwe methode voor zowel maxima en minima, als voor raaklijnen, ..., en een opmerkelijk soort rekenmechanisme daarvoor*; zijn oplossing van het quadratuurprobleem, leidend tot onze integraalrekening, verscheen twee jaar later.

Newton or Leibniz?

Als het gaat om de uitvinding van de differentiaal- en integraalrekening, wordt Leibniz altijd in één adem genoemd met Newton. Isaac Newton (1643–1727) had al in de jaren 1665–66, dus 10 jaar eerder dan Leibniz, een methode ontdekt (de *Method of fluxions*) met dezelfde mogelijkheden als de *Nova methodus* van Leibniz.

In 1673 en in 1676 bezocht Leibniz Londen o.a. om daar een door hem in Parijs vervaardigde rekenmachine te demonstreren. In Londen circuleerden echter handgeschreven teksten met Newton's ideeën. Leibniz kan dus op de hoogte zijn geweest van Newton's vinding, of wellicht erdoor geïnspireerd zijn. Dat was althans de mening van veel Engelse wiskundigen. Zij hebben dan ook aan het einde van de 17e eeuw tientallen jaren verbitterd gevochten om Leibniz als dief ontmaskerd te krijgen.

Tegenwoordig neemt men echter aan dat de methode van Leibniz onafhankelijk van die van Newton is ontstaan. In elk geval was Leibniz Newton voor met publiceren. Leibniz deed dat in 1684 en 1686. Newton volgde in 1687. De huidige opzet van de differentiaal- en integraalrekening, inclusief de gebruikte notaties, is gebaseerd op de methode van Leibniz.

Gelukkig ■ ■ ■ ■ ■ □ □ □ □ □ □ □

In zijn Parijse jaren heeft Leibniz ook uitgebreide en tot op zekere hoogte succesvolle pogingen ondernomen om een mechanische rekenmachine te bouwen.

In 1679 voerde hij de notatie van getallen met de cijfers 1 en 0 in. Bovendien gaf hij zelfs aan, hoe je een rekenmachine zou kunnen bouwen die op basis van dit tweetallig talstelsel werkte. De machine is helaas nooit gebouwd.

En nu weer terug naar het jaartal 1984.

Om 1984 in het tweetallig stelsel te krijgen, moet je het opsplitsen in machten van twee. Dus

$$1984 = 1824 + 512 + 256 + 128 + 64 = \\ 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + \\ 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0,$$

zodat 1984 in het tweetalig stelsel geschreven wordt als 11111000000! Zou Leibniz deze bijzonderheid van 1984 niet onmiddellijk toegegeven hebben bij het zien van bovenstaande nieuwjaarswens voor het jaar 1984?

15 Martij 1679.

De Progressione Dyadica - Pars I.

Numeratio

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010	11011	11100	11101	11110	11111	100000

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
10001	10010	10011	10100	10101	10110	10111	11000	11001	11010	11011	11100	11101	11110	11111	100000

Pl. 11111
 100000
 100001
 100000
 100001
 100011
 100100
 100101
 100110
 100111
 101000
 101001
 101010
 101011
 101100
 101101
 101110
 101111
 110000
 110001
 110010
 110011
 110100
 110101
 110110
 110111
 111000
 111001
 111010
 111011
 111100
 111101
 111110
 111111

Adscripta progressio facile continuari potest. A dextra finis habetur, ubi subscripta sunt 0. donec occurrat in superstante etiam 0. Subscribitur I. sequens ut ultra pergi opus, nam reliqua praecedere non possunt. Ita ex 1010111 87
 1011.000 88
 idem est a finitioribus: 1011000 esse $2^6 + * + 2 + 2^3 + * * *$
 64 + 16 + 8

Het begin van Leibniz' handschrift 'De progressionibus arithmetico-geometricis'

Het begin van Leibniz' handschrift 'De progressionem dyadica' over het tweetallig stelsel.

88
Fundament

12. *Pygospio* Bivalve
 13. *Pygospio* Bivalve
 14. *Pygospio* Bivalve
 15. *Pygospio* Bivalve
 16. *Pygospio* Bivalve
 17. *Pygospio* Bivalve
 18. *Pygospio* Bivalve
 19. *Pygospio* Bivalve
 20. *Pygospio* Bivalve
 21. *Pygospio* Bivalve
 22. *Pygospio* Bivalve
 23. *Pygospio* Bivalve
 24. *Pygospio* Bivalve
 25. *Pygospio* Bivalve
 26. *Pygospio* Bivalve
 27. *Pygospio* Bivalve
 28. *Pygospio* Bivalve
 29. *Pygospio* Bivalve
 30. *Pygospio* Bivalve
 31. *Pygospio* Bivalve
 32. *Pygospio* Bivalve
 33. *Pygospio* Bivalve
 34. *Pygospio* Bivalve
 35. *Pygospio* Bivalve
 36. *Pygospio* Bivalve
 37. *Pygospio* Bivalve
 38. *Pygospio* Bivalve
 39. *Pygospio* Bivalve
 40. *Pygospio* Bivalve
 41. *Pygospio* Bivalve
 42. *Pygospio* Bivalve
 43. *Pygospio* Bivalve
 44. *Pygospio* Bivalve
 45. *Pygospio* Bivalve
 46. *Pygospio* Bivalve
 47. *Pygospio* Bivalve
 48. *Pygospio* Bivalve
 49. *Pygospio* Bivalve
 50. *Pygospio* Bivalve
 51. *Pygospio* Bivalve
 52. *Pygospio* Bivalve
 53. *Pygospio* Bivalve
 54. *Pygospio* Bivalve
 55. *Pygospio* Bivalve
 56. *Pygospio* Bivalve
 57. *Pygospio* Bivalve
 58. *Pygospio* Bivalve
 59. *Pygospio* Bivalve
 60. *Pygospio* Bivalve
 61. *Pygospio* Bivalve
 62. *Pygospio* Bivalve
 63. *Pygospio* Bivalve
 64. *Pygospio* Bivalve
 65. *Pygospio* Bivalve
 66. *Pygospio* Bivalve
 67. *Pygospio* Bivalve
 68. *Pygospio* Bivalve
 69. *Pygospio* Bivalve
 70. *Pygospio* Bivalve
 71. *Pygospio* Bivalve
 72. *Pygospio* Bivalve
 73. *Pygospio* Bivalve
 74. *Pygospio* Bivalve
 75. *Pygospio* Bivalve
 76. *Pygospio* Bivalve
 77. *Pygospio* Bivalve
 78. *Pygospio* Bivalve
 79. *Pygospio* Bivalve
 80. *Pygospio* Bivalve
 81. *Pygospio* Bivalve
 82. *Pygospio* Bivalve
 83. *Pygospio* Bivalve
 84. *Pygospio* Bivalve
 85. *Pygospio* Bivalve
 86. *Pygospio* Bivalve
 87. *Pygospio* Bivalve
 88. *Pygospio* Bivalve
 89. *Pygospio* Bivalve
 90. *Pygospio* Bivalve
 91. *Pygospio* Bivalve
 92. *Pygospio* Bivalve
 93. *Pygospio* Bivalve
 94. *Pygospio* Bivalve
 95. *Pygospio* Bivalve
 96. *Pygospio* Bivalve
 97. *Pygospio* Bivalve
 98. *Pygospio* Bivalve
 99. *Pygospio* Bivalve
 100. *Pygospio* Bivalve

Correspondentie

Wanneer je wilt reageren op Pythagoras, of melding wilt maken van je ervaringen met wiskunde, kun je je bijdrage richten aan het redactiesecretariaat. Vermeld daarbij de naam van je school en je klas.

Wie heeft gelijk?

In nummer 3 van de vorige jaargang vroegen we wie een behoorlijke schatting kon geven van het aantal cijfers van het reuzengetal

$5!^{5!^{5!^{5!^{5!}}}}$, ofwel van $120^{120^{120^{120^{120}}}}$ immers $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.

Even terzijde, dit getal was afkomstig uit het artikel 'De 5 vijven' waarin de resultaten werden besproken van de 5-vijven-wedstrijd: zoveel mogelijk getallen schrijven met 5 vijven.

Uit de reacties hebben we de onderstaande geselecteerd. Je ziet dat de schrijvers, Freek Bomhof en Carlo Delhez, allebei een overtuigend verhaal hebben, maar... het helemaal niet met elkaar eens zijn.

We vinden dat te leuk om als scheidsrechter op te treden. Leg het maar eens voor aan je eigen wiskundeleraar!

Freek en Carlo zullen ook over de uitkomst van 3^{3^3} wel van mening verschillen. Wat krijgt Freek eruit? En Carlo?

Waarom zijn ze het wél eens over 2^{2^2} ?

Gewoon uitrekenen!

U vroeg wie een behoorlijke schatting kon maken van het aantal cijfers van een groot getal.

Welnu, dat hoeft niet eens te worden geschat. Dat kun je gewoon uitrekenen!

De truuk is als volgt: je neemt $^{10}\log$ van het getal, streept de decimalen weg, en telt er één bij op. Ga maar na met bijvoorbeeld 999 en 1000.

Het aantal cijfers van het getal bedraagt nu:

$$^{10}\log 120^{120^{120^{120^{120}}}} = 120^4 \cdot ^{10}\log 120$$

Met de rekenmachine kwam ik uit op 431139024 (!) Een krant die dit getal zou willen uitschrijven en publiceren, zal een jaar lang elke dag een bijlage van ca. 100 pagina's moeten geven!

Freek Bomhof A6b, de Heertganck, Heerde

Onmetelijk groot

Hierbij wil ik even reageren op het in het derde nummer van Pythagoras opgenomen artikelje 'De 5 vijven'. Daarin werd gevraagd om een behoorlijke schatting van het aantal cijfers van

$$s = 120^{120^{120^{120^{120}}}}$$

te geven.

U besepte waarschijnlijk echter niet hoe immens groot dit getal wel niet is!

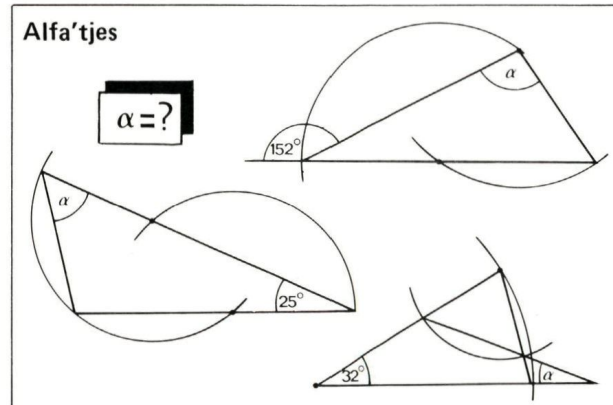
Stel je $a = 120^{120^{120^{120^{120}}}}$, dan moet je dus het aantal cijfers van $s = 120^a$ berekenen. Dat kan gemakkelijk gedaan worden door te schrijven:

$$120^a = (10^{^{10}\log 120})^a = 10^{a \cdot ^{10}\log 120}$$

Het aantal cijfers van 10^p is $p+1$ (bijvoorbeeld 10^2 heeft $2+1=3$ cijfers, 10^3 heeft er 4, enz.). Daarom is het aantal cijfers van 120^a gelijk aan het gehele deel van $a \cdot ^{10}\log 120 + 1$. En daar

$a = 120^{120^{120^{120^{120}}}}$, is dus zelfs het getal dat het aantal cijfers van s moet weergeven onmetelijk groot. Kun je nagaan hoe groot s zelf is!

Carlo Delhez 5 vwo, Steenberg



Eén metertje meer...

Stel de aarde voor als een volkomen gladde bol met een straal van 6378 km. Langs de evenaar is een touw strak gespannen. De lengte ervan is $2\pi \times 6378$ km.

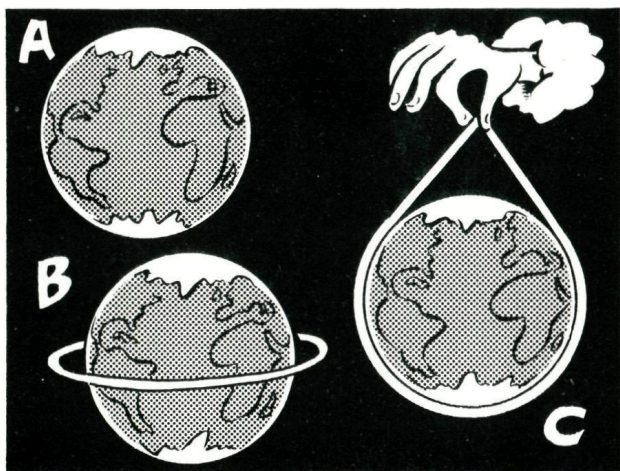
Wanneer je nu dat touw overal precies één meter boven het aardoppervlak wilt hebben, hoeveel kilometer touw heb je dan méér nodig?

Het antwoord is: helemaal geen kilometers, maar iets meer dan 6 meter!

Reken maar mee! Zeg dat de straal van de aarde r meter is. Dan is de lengte van het oorspronkelijke touw $2\pi r$ meter. Het nieuwe touw vormt een cirkel met een straal van $r + 1$ meter. De omtrek wordt dus $2\pi(r + 1)$. Het verschil is dan 2π meter $\approx 6,28$ meter. Je ziet trouwens dat het niets uitmaakt of je dat nu bekijkt voor de aarde, de maan, een voetbal of een sinaasappel. Steeds heb je 6,28 meter extra touw nodig dig, als je de straal 1 meter groter maakt.

De aarde opgehangen

Maar nu iets anders. Maak het (strak rond de aarde gespannen) touw één meter langer. Stel je voor dat een reus de aarde met dat touw aan één punt optilt (en dat het touw daarbij niet uitrekt!). Hoeveel meter zal dat punt dan boven het aardoppervlak komen?

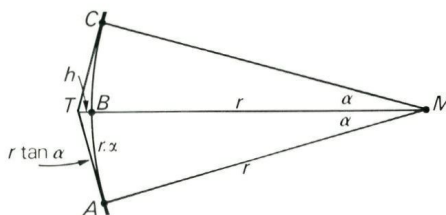


Touw strak om de aarde (A), zes meter langer en het komt één meter boven de oppervlakte (B), één meter langer en je hangt de aarde eraan op (C).

Gezien de totale lengte van de aardomtrek is die ene meter extra natuurlijk maar een schijntje, dus erg hoog kan dat punt niet komen, denk je misschien.

Maar daar kun je je lelijk in vergissen. Reken maar weer mee!

Hieronder zie je een situatieschets. Het touw wordt bij T opgetild. Bij A en C komt het weer op aarde terecht. M is het middelpunt van de aarde, r de straal, dus $r = 6378000$ m. B is het punt op aarde recht onder T , en $h = BT$ is de te berekenen hoogte.



We geven hoek AMT aan met α . Als we α uitdrukken in radialen, is de lengte van boog AB – dus de afstand van A en B langs het aardoppervlak – gelijk aan $r\alpha$. Verder is $AT = \tan\alpha$, en omdat $AT + TC$ een meter langer is dan boog ABC , geldt (delen door 2):

$$r \tan \alpha - r\alpha = \frac{1}{2}, \text{ dus } \tan \alpha - \alpha = \frac{1}{2r}. \quad (1)$$

Verder zie je dat $\cos \alpha = \frac{r}{r+h}$, en dat kun je omwerken tot $h = r \{ (1/\cos \alpha) - 1 \}$

$$\text{ken tot } h = r \{ (1/\cos \alpha) - 1 \} \quad (2)$$

Aan vergelijking (1) zie je dat $(\tan \alpha - \alpha)$ verschrikkelijk klein is (want $r = 6378000$). Dat betekent (denk aan de grafiek van de tangensfunctie) dat ook hoek α zelf ontzettend klein moet zijn.

Nu geldt voor kleine waarden van α :

$$\frac{\tan \alpha - \alpha}{\alpha} \approx \frac{1}{3} \text{ en } \frac{(1/\cos \alpha) - 1}{\alpha^2} \approx \frac{1}{2}.$$

Toets het maar eens in op je rekenmachine (denk eraan in radialen werken!). Zesdeklidders kunnen de juistheid van die benaderingen misschien ook bewijzen met limieten en de regel van De L'Hospital.

In elk geval kunnen we zonder merkbare fouten te maken (1) en (2) vervangen door

$$\frac{\alpha^3}{3} = \frac{1}{2r} \quad (1') \quad \text{en } h = r \frac{\alpha^2}{2} \quad (2')$$

Dit geeft samen $h = \frac{r}{2} \left(\frac{3}{2r} \right)^{2/3} = 121,50..$ m. En daar past de domtoren uit Utrecht met z'n 112 meter nog ruim onder!

Pythagoras Olympiade



Al een paar jaar draait in Pythagoras een wedstrijd voor wiskunde-bollebozen: de Pythagoras Olympiade. Het gaat om opgaven — drie in elk nummer — waarvoor je nauwelijks wiskundige voorkennis nodig hebt. Tot ruim een maand na de verschijningsdatum kun je oplossingen insturen.

Prijzen Iedere opgave is een wedstrijd op zichzelf. Je hoeft niet aan alles mee te doen, je kunt van elke som afzonderlijk een oplossing inzenden. Bij elke opgave verloten we onder de goede inzenders twee prijzen van f 10,—/Bfr 150. Verder vormen de 12 opgaven van één jaargang een *ladderwedstrijd*. Iedere goede oplossing geeft 1 punt. De drie inzenders met de meeste punten krijgen elk een prijs van f 25,—/Bfr 400. Bovendien ontvangen de beste tien van de ladderwedstrijd een uitnodiging voor de Tweede Ronde (tevens finale) van de NEDERLANDSE WISKUNDE OLYMPIADE, zelfs al hebben ze niet aan de Eerste Ronde meegedaan of daarbij niet voldoende punten behaald.

Oplossingen De uitwerkingen komen natuurlijk in Pythagoras. Bij elke opgave wordt de oplossing van één van de inzenders gepubliceerd. Maar gezien de benodigde correctietijd en de productietermijn van Pythagoras zal dat meestal in de volgende jaargang kunnen gebeuren. Maar... je kunt de uitslag en de uitgekozen oplossing eerder krijgen als je een aan jezelf geadresseerde en gefrankeerde enveloppe meestuurt.

Inzendingen Leerlingen van het voortgezet/secundair onderwijs kunnen hun oplossingen insturen aan: *Pythagoras Olympiade, Cornelis Krusemanstraat 60^{II}, 1075 NS Amsterdam*. De inzendtermijn voor de eerste drie opgaven, die op pagina 22 staan, sluit op **1 januari 1985**. Vermeld op elk (éénzijdig beschreven) vel: naam, adres, geboortedatum, school, schooltype en klas. Verder moet elke oplossing op een nieuw vel beginnen. We bekijken alleen goed leesbare oplossingen die volledig uitgewerkt zijn, met verklarende tekst in goed lopende zinnen.

Uitslag ladderwedstrijd

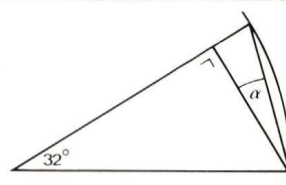
Aan de Pythagoras Olympiade uit de vorige jaargang hebben in totaal 68 leerlingen meegedaan. Dat is wat minder dan gebruikelijk. Dat is waarschijnlijk veroorzaakt doordat we wat organisatorische problemen hebben gehad. Bij de verzending van nummer 2 gooide de poststaking namelijk roet in het eten, en daardoor kwamen ook de nummers 3 en 4 veel later uit dan de bedoeling was. De inzendtermijnen waren dus wat krap; onze excuses! Niettemin kregen we veel goede oplossingen binnen. De uitslag van de ladderwedstrijd is:

1/4	Jan de Boer	
	6 vwo, RSG Magister Alvinus, Sneek	12 p
	Roelant Nieboer	
	6 g, Herman Wesselink College, Amstelveen	12 p
	Dirk Ophoff	
	5 vwo, Gomarus College, Groningen	12 p
	Menke Ubbens	
	6 vwo, RSG Magister Alvinus, Sneek	12 p
5	Willem Brussaard	
	5 havo, van Lodenstein SG, Amersfoort	11 p
6	Wiebe Kees Goodijk	
	6 g, Christelijk Gymnasium, Leeuwarden	10,5 p
7/8	Ben Moonen	
	5 vwo, St. Janscollege, Hoensbroek	10 p
	Frank Robijn	
	6 vwo, RSG Koning Willem II, Tilburg	10 p
9	Danny ten Haaf	
	4 vwo, Dominicus College, Nijmegen	9,5 p
10	Floor van Lamoën	
	6 g, Stedelijk Gymnasium, Leeuwarden	9 p

Zoals je ziet, waren er 4 deelnemers met het maximale aantal punten. In de reglementen staat dat de drie besten van de ladder een boekenbon krijgen van f 25,—. We hebben in dit geval maar besloten ze er alle vier een te geven. Proficiat!

Alfa'tje

$\alpha = ?$





Geheimschrift I

Geheimschrift, een spelletje?

Je zult er vast wel eens aan mee gedaan hebben, of althans gemerkt hebben dat anderen er mee bezig waren: briefjes aan elkaar doorgeven, waarop een boodschap stond die in geheimschrift geschreven was.

Achteraf vind je dat misschien wat flauw. Toch wordt dit bijvoorbeeld door militairen, diplomaten, geheime diensten e.d. heel serieus bedreven. In die kringen komt het vaak voor dat bepaalde berichten slechts voor een paar ingewijden bestemd zijn.

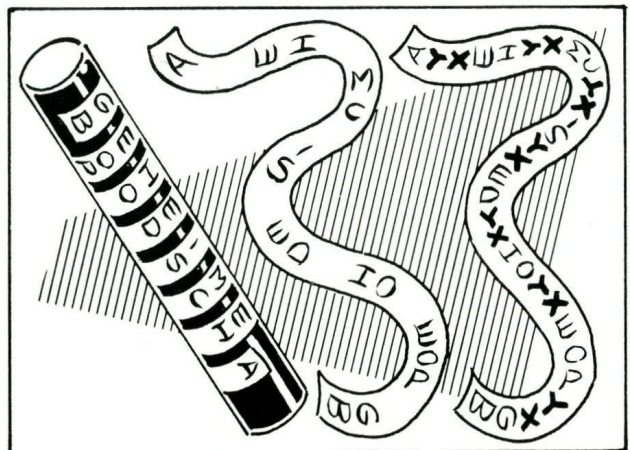
Maar om die berichten op de plaats van bestemming te krijgen, moet men zich meestal van openbare communicatiekanalen zoals de post, de telefoon e.d. bedienen. Voor een buitenstaander die daaraan veel waarde hecht, is het dan ook niet moeilijk om dergelijke berichten te onderscheppen. Daarom worden ze meestal in geheimschrift geschreven, zodat ingeval iemand ze weet te onderscheppen, hij nog geen kennis kan nemen van de inhoud. Tenzij hij natuurlijk weet hoe dat geheimschrift in elkaar zit, of daarachter weet te komen!

Voor de laatste jaren staat de **cryptologie**, de leer van het geheimschrift, sterk in de belangstelling. De

talloze gegevens die tegenwoordig in veel computersystemen zijn opgeslagen, zijn namelijk lang niet voor iedereen bestemd. Daarom wordt daarbij in toenemende mate geheimschrift toegepast. De cryptologie is dan ook uitgegroeid tot een aparte tak van de wetkunde.

De cryptologie wordt opgesplitst in twee delen: de **cryptografie**, het ontwerpen van geheimschriften, en de **crypto-analyse**, het ontcijferen van geheimschriften. Maar omdat vooral de laatste jaren de nadruk op de cryptografie ligt, wordt die term tegenwoordig ook voor het hele gebied van de cryptologie gebruikt.

In dit eerste van een serie artikelen over geheimschrift gaan we eens kijken naar enkele voorbeelden. Daaruit zal blijken dat er al zo'n 2000 jaar serieus met geheimschrift wordt omgesprongen. Ook zul je aan de hand van die historische voorbeelden alvast een beetje worden 'ingewijd' in de geheimen van de cryptologie.



Al in 400 v.C. gebruikten de Spartanen de scytale. Dit is een strook papier die in een spiraal rond een stokje wordt gewikkeld. Het bericht wordt over de lengte van het stokje op het papier geschreven. Daarna wordt de strook afgewikkeld en kan door een looper naar zijn bestemming worden gebracht. Wanneer de ontvanger de strook om een even groot stokje wikkelt kan hij het bericht lezen.

Afgewikkeld vertoont de strook enkele letters op een bepaalde afstand. De ruimten tussen deze letters kunnen eventueel met willekeurige andere letters (zoals hier bijvoorbeeld steeds met X en Y) worden opgevuld.

Het caesaralfabet

Naar verluidt, wisselden de oude Romeinen geheime berichten uit door het hoofd van een slaaf kaal te scheren, de boodschap op zijn hoofdhuid te schrijven, en de slaaf op pad te sturen, nadat zijn haar weer was gegroeid.

Dit was misschien wel slim, maar heeft natuurlijk niets te maken met het ontwerpen en ontcijferen van geheimschrift.

Een serieuzer cryptografische systeem werd gebruikt door de Romeinse keizer Julius Caesar (100–44 v.C.). Het wordt daarom **caesaralfabet** genoemd. Daarbij wordt elke letter uit de oorspronkelijke tekst, de **klare tekst**, vervangen door een letter die drie plaatsen verder in het alfabet staat. De tekst die dan ontstaat, het eigenlijke geheimschrift dus, wordt de **cijfertekst** genoemd.

Het omwerken van de klare tekst tot de cijfertekst, heet **vercijferen**. De bewerking die je daarbij toe moet passen, heet de **sleutel**. Bij het geheimschrift van Caesar is de sleutel dus: *vervang elke letter door een letter die drie plaatsen verder in het alfabet staat*.

Onder **ontcijferen** verstaat men het omwerken van een cijfertekst tot een klare tekst. De bewerking die je nodig hebt om dat uit te voeren, heet de **contra-sleutel**.

Je ziet dat wanneer je bij zo'n systeem als dat van Caesar, de sleutel eenmaal weet, de contrasleutel daar gemakkelijk uit is af te leiden (*elke letter uit de cijfertekst vervangen door een letter die drie plaatsen eerder in het alfabet staat*). Dit geldt overigens voor bijna alle 'klassieke' systemen, zoals je in de andere voorbeelden ook zult zien.

We zullen hier een eenvoudige toepassing geven van het caesaralfabet. Bedenk daarbij wel dat Caesar natuurlijk het Romeinse alfabet gebruikte, wat wij hier maar niet zullen doen.

klare tekst: I K KWAM I K ZAG I K OVERWON
cijfertekst: L N N Z D P L N C D J L N R Y H U Z R Q

In dit voorbeeld zie je ook meteen dat er geen onderscheid gemaakt wordt tussen hoofd- en kleine letters. Verder wordt er meestal niet gelet op leestekens en spaties (ruimten tussen de woorden). En dikwijls wor-

den de letters van de cijfertekst in groepjes van vijf bij elkaar gezet.

Dus eigenlijk moet de cijfertekst er uitzien als:

cijfertekst: LNNZD PLNCD JLNRY HUZRQ

Misschien heb je je al afgevraagd waarom Caesar nu juist een verschuiving van drie letters heeft genomen. Daarover is niets bekend. Maar inderdaad, je had net zo goed een verschuiving van bijvoorbeeld tien of veertien letters kunnen nemen.

In het algemeen wordt dan ook een verschuiving van n letters een **caesaralfabet** genoemd.

Ontcijfering Een cijfertekst omzetten in een klare tekst is niet zo moeilijk, als je tenminste weet dat je te maken hebt met een caesaralfabet.

Je kunt dan gewoon alle 25 mogelijke verschuivingen proberen. De verschuiving die dan een zinnige klare tekst oplevert, zal ongetwijfeld de juiste zijn.

Weet je bovendien nog in welke taal (Nederlands, Frans, Duits of Engels om maar wat te noemen) de klare tekst moet komen, dan kun je kijken welke letter het meest voorkomt in de cijfertekst. Deze letter zal naar alle waarschijnlijkheid overeenkomen met de meest voorkomende letter in de gewone taal (in het Nederlands en het Engels de letter e). Daarmee weet je met welke verschuiving je te doen hebt, en is de zaak in principe opgelost. Je hoeft dan dus niet meer alle 25 mogelijkheden uit te proberen.



Ingewikkelder systemen

Bij het caesaralfabet werd alleen maar een verschuiving van de letters toegepast. Je kunt natuurlijk ook de 26 letters van het alfabet willekeurig van plaats verwisselen. Je hebt dan niet meer 26 mogelijke sleutels, maar $26!$ ($26 \text{ faculteit} = 26 \cdot 25 \cdot 24 \cdot \dots \cdot 3 \cdot 2 \cdot 1$) mogelijke sleutels.

Het is natuurlijk onbegonnen werk om die allemaal na te gaan. En je zou dus geneigd zijn te veronderstellen dat je zo een cijfertekst kunt maken die nauwelijks te ontcijferen is, als je de sleutel niet weet.

Maar schijn bedriegt. Ook hier kom je door te tellen hoe vaak bepaalde letters in de cijfertekst voorkomen, al een heel eind.

Als je dan ook nog handig gebruik weet te maken van de kenmerken van de taal waarin de klare tekst is geschreven, is ontcijfering niet al te moeilijk meer. Het geheimschrift uit het verhaal van Poe dat verderop wordt behandeld, is daar een goed voorbeeld van.

De methode van de Vigenère

In 1586 dacht de Fransman Blaise de Vigenère een systeem uit waarbij op de achtereenvolgende letters van de klare tekst steeds een andere verschuiving werd toegepast. Dus bijvoorbeeld een verschuiving van 2 plaatsen voor de eerste letter, een van 6 plaatsen voor de tweede letter, een van 18 plaatsen voor de derde letter en dan weer van voren af aan.

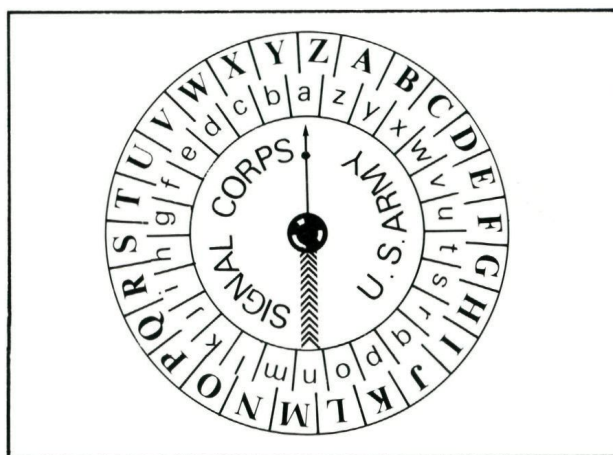
De sleutel wordt dan gegeven door de opeenvolgende verschuivingen; hier de getallen 2, 6 en 18.

Deze getallen worden in de vorm van een **sleutelwoord** gegeven. Dit sleutelwoord wordt steeds maar herhaald onder de klare tekst. Bijvoorbeeld:

Klare tekst: **pytha goras iseen leukt ijdsc hrift**

sleutel: *gehei mgehe imgeh eimge heimg eheim*

Nu geven de letters van *geheim* steeds de verschuiving aan van de bovenstaande letters uit de klare tekst. Ga daartoe uit van de eerste letter, de a, van het alfabet. Om bij de letter g te komen moet je de a 6 plaatsen verschuiven, om bij de e te komen 4 plaatsen, om bij de h te komen 7 plaatsen, om bij de i te komen 8 plaatsen en om bij de m te komen 12 plaatsen. Daarmee geeft het sleutelwoord *geheim* dus de volgende



Jaren geleden werden in het Amerikaanse leger bij het vercijferen en ontcijferen van teksten cijferwielen gebruikt. Op het buitenste wiel stond het alfabet van de klare tekst, op het verwisselbare binnenste dat van de cijfertekst (hier in omgekeerde volgorde).

opeenvolgende verschuivingen aan: 6, 4, 7, 4, 8, 12.

Dan kunnen we nu de cijfertekst maken.

Klare tekst: **pytha goras iseen leukt ijdsc hrift**

sleutel: *gehei mgehe imgeh eimge heimg eheim*

Cijfertekst: **vcali suvhw qekiu pmgqx pnlei lymnf**

Als je het sleutelwoord weet, is het ontcijferen geen kunst. Je zet namelijk het sleutelwoord steeds maar boven de cijfertekst en voert aan de hand daarvan verschuivingen in omgekeerde richting uit.

Hier hebben we nog maar een kort sleutelwoord gebruikt, maar je zult wel willen aannemen dat wanneer je een lang sleutelwoord gebruikt, of zelfs een hele zin, ontcijferen een heel karwei is.

Heel lang, tot ca. 1860, heeft men gedacht dat de vigenère niet te ontcijferen was, wanneer het sleutelwoord niet bekend was. Een cijfertekst die volgens deze methode tot stand was gekomen, werd dan ook als absoluut veilig beschouwd.

Omstreeks 1860 ontwikkelde de Duitser Kasiski een methode om de lengte van het sleutelwoord te bepalen. En toen was er weinig meer voor nodig om de vigenère te kunnen ontcijferen. Maar daar zullen we hier niet meer op ingaan.

De zwarte magie van Vieta

Hoewel hij rechtsgeleerde was, gaat François Viète (1540–1603), wiens Latijnse naam Vieta was, door voor één van de grootste Franse wiskundigen uit de 16e eeuw. Hij was korte tijd raadsman van Koning Hendrik III, viel in ongenade, maar werd door Hendrik IV weer tot raadsman benoemd.

Nu ondervond Hendrik IV nogal wat tegenwerking van Philips II, koning van Spanje. Vanaf zeker moment wist hij echter beslag te leggen op cryptografische berichten van Philips II. Deze waren bestemd voor de Nederlanden, die toen door Philips II werden geregeerd, maar zich van hem probeerden te ontdoen (Tachtigjarige Oorlog).

Je begrijpt dat Hendrik IV er veel voor over had om achter de inhoud van die berichten te komen. Daarom gaf hij ze aan Vieta, en deze slaagde erin om die cijferteksten te ontcijferen. Dit ging enkele jaren goed. Er kwam een einde aan toen Vieta tegen de ambassadeur van Venetië vertelde dat hij geheime berichten van Philips II kon ontcijferen. Dit nieuwtje ging snel rond en bereikte natuurlijk ook Philips II. Die liet uiteraard terstond de sleutel veranderen.

Maar dat niet alleen. Hij was er zo verbolgen over dat zijn geheime code die hij voor onbreekbaar hield, gebroken was, dat hij zich tot de Paus wendde.

Met de bedoeling Vieta veel last te bezorgen, vertelde hij tegen de Paus dat Vieta **zwarte magie** had gebruikt bij de ontcijfering van het geheimschrift. Daarop moet de Paus wat binnensmonds gelachen hebben, want zijn eigen raadsliden waren er al veel eerder in geslaagd om de geheime berichten van Philips II te ontcijferen!

De binaire code van Francis Bacon

In 1605 maakte de Engelse staatsman en geleerde Sir Francis Bacon (1561–1626) in zijn boek 'Of the advancement of learning' melding van een methode die hij voor zijn geheime diplomatieke boodschappen gebruikte.

Enige tijd later, in 1623, beschreef hij die volledig in zijn 'De augmentis scientiarum'. Daaruit blijkt bovendien dat dit ook het allereerste geheimschrift is dat werkt volgens een binaire code. Om dat in te kunnen zien moet je eerst weten hoe dat geheimschrift van Bacon in elkaar zit.

A 1 DIT IS EEN GEHEIM BERICHT
 2 D T S E G H I B R C H T
 3 DTSEGHIBRCT IIENEEMEIH

A Bij de hekode of rail fence worden de oneven en even letters van de klare tekst (1) gesplitst door ze in twee regels op te schrijven (2). De cijfertekst (3) wordt dan verkregen door de bovenste en de onderste regel achter elkaar te zetten.

B Bij routetranspositie zet men de letters van de klare tekst (1) in een bepaalde volgorde onder elkaar (2). De cijfertekst (4) verkrijgt men dan door ze, gelezen volgens een andere route (3), weer achter elkaar te zetten.

B 1 DIT IS EEN GEHEIM BERICHT
 2 DITISEE
 MEHEGN
 BERTCHT
 3 DITISEE
 MEHEGN
 BERTCHT
 4 DMBEITERIHGEENT

C Bij het Rozenkruisersgeheimschrift (ook wel pigpen of varkenshok geheten) vormt 1 de sleutel. Bij verticijfering wordt elke letter uit de klare tekst vervangen door het hokje waar hij in staat met een punt op de plaats die hij in dat hokje inneemt (2). Probeer de aldus verkregen cijfertekst (3) maar eens te ontcijferen! Je komt ook wel variaties (zoals 4) op de sleutel (1) tegen. Bij deze variant (4) wordt in de cijfertekst elke letter uit de klare tekst vervangen door een leeg hokje of door een hokje met een punt erin (5).

A	B	C	D	E	F	G
aaaaa	aaaab	aaaba	aaabb	aabaa	aabab	aabba
H	I	K	L	M	N	O
aabbb	abaaa	abaab	ababa	ababb	abbaa	abbab
P	Q	R	S	T	U	W
abbbba	abbbb	baaaa	baaab	baaba	baabb	babaa
X	Y	Z				
babab	babba	babbb				

C 1			2	A = 	V =
	ABC	DEF		B = 	W = 
	J K L	M N O		C = 	X = 
	S T U	V W X		D = 	Y = 
		Y Z		E =	Z = 

3

[A sequence of 16 boxes containing symbols: Uppercase letters A through P.]

4

A	B	C
D	E	F
G	H	I
N	O	P
Q	R	S
T	U	V



5

A = 

B = 

C = 

D = 

E = ...

V =

W = 

X = 

Y = 

Z = 

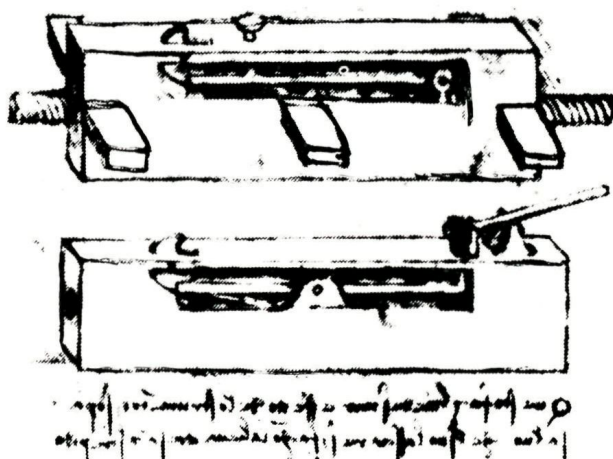
Binaire code Getallen en letters (tekens dus) worden in computers voorgesteld door een groepje nullen en enen. Nu verving Bacon elke letter uit de klare tekst door een groepje van vijf a's en b's. Maar hij had natuurlijk ook in plaats van een a een 0 kunnen nemen, en in plaats van een b een 1. Elke letter uit de klare tekst zou dan kunnen worden vervangen door een groepje van vijf nullen en enen. Dat zou dan het volgende resultaat geven:

A	B	C	D	E	F	G
00000	00001	00010	00011	00100	00101	00110
H	I	K	L	M	N	O
00111	01000	01001	01010	01011	01100	01101
P	Q	R	S	T	U	W
01110	01111	10000	10001	10010	10011	10100
X	Y	Z				
10101	10110	10111				

Het woord 'flee' uit de klare tekst zou dan dus op de volgende manier worden omgezet:

FLEE → 00101 01010 00100 00100

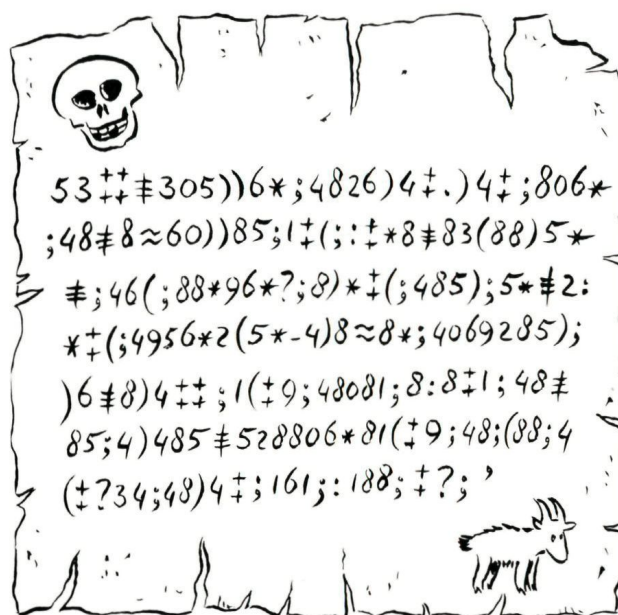
Ofwel in 00101010100010000100, en zo'n rijtje nullen en enen is gemakkelijk door computers te verwerken. Bij het ontcijferen moet je dat rijtje dan uiteraard weer opdelen in groepjes van vijf!



Om diefstal van zijn uitvindingen te voorkomen schreef Leonardo da Vinci (1452–1519) de teksten bij zijn ontwerpen in spiegelschrift.

Geheimschrift bij Edgar Allan Poe

De Amerikaanse schrijver Edgar Allan Poe (1809–1849) schreef in 1843 het verhaal 'The gold bug' (in het Nederlands vertaald als 'De gouden skarabee' of 'De gouden kever'). Daarin komt een zekere William Legrand voor, die op een wonderlijke manier een stuk perkament in handen heeft gekregen. Daarop staat een stuk geheimschrift (zie figuur), dat hij maar al te graag ontcijferen wil. Uitvoerig beschrijft Poe hoe Legrand dat aanpakt. We zullen kijken hoe dat gaat.



Het doodshoofd zegt hem dat hij te maken moet hebben met zeerovers.

Het bokje beschouwt hij als een ondertekening in de vorm van een hiëroglief. Maar van wie?

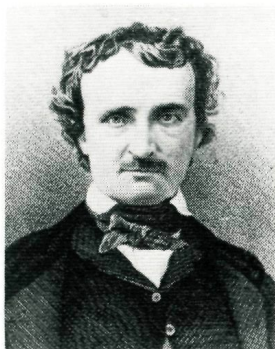
Wel, na enig nadenken komt Legrand op het idee dat dit op een of andere kapitein Kidd (kid is het Engelse woord voor bokje) moet slaan. Daarmee is het voor hem ook meteen duidelijk dat de klare tekst in het Engels geschreven is.

Nu blijkt echter uit de cijfertekst dat er tussen de woorden geen spaties staan. Dus Legrand kan niet na gaan of er soms één-letterige woorden in de cijfertekst voorkomen, zodat hij bijvoorbeeld niet kan achterhalen welk teken er gebruikt is voor 'a' en 't' (Denk eraan dat de klare tekst in het Engels moet komen!).

Ontcijfering Eerst gaat Legrand na hoe vaak elk teken in de cijfertekst voorkomt. Dat geeft het volgende resultaat (Tel maar na!):

Het teken 8 komt 33 keer voor

;	26
4	19
+ en)	16
*	13
5	12
6	11
(	9
# en 1	8
0	6
9 en 2	5
: en 3	4
?	3
≈	2
— en .	1



E. A. Poe

Nu weet Legrand dat in het Engels de letter e het meest voorkomt, en dat daarop respectievelijk a o i d h n r s t u y c f g l m w v b k p q x z en j volgen.

Hij gaat er daarom maar vanuit dat het meest voorkomende teken, de 8, staat voor de letter e.

In het Engels komt het woord 'the' het meest voor. Ook dat weet Legrand, daarom gaat hij kijken of dezelfde groep van drie tekens in gelijke volgorde meer malen voorkomt met aan het einde het cijfer 8.

Hij vindt zeven keer zo'n groep, namelijk ;48. En hij neemt dan ook aan dat ; de t is en 4 de h. Bovendien kan hij nu ook aangeven met welk teken sommige woorden beginnen of eindigen. Daartoe gaat hij deze drie bekende letters in de hele reeks invullen, en kijkt naar de op één na laatste plaats waar de serie ;48 voorkomt.

De ; die daar achter staat, moet dan het begin van een woord zijn, en van de vijf tekens achter die ; kent hij er al vier!

Achter de op één na laatste keer dat ;48 voorkomt, staan dus zes tekens waarvan er al vijf bekend zijn.

Ga maar na. Er staat ;(88;4 of na invulling van de bekende tekens: t eeth met een open plek voor het nog onbekende teken.

Nu blijkt dat de 'th' niet aan het einde kan staan van een woord dat begint met 't ee'. Want welke letter

van het alfabet je ook op de open plaats invult, je vindt geen enkel Engels woord dat er uit kan zien als 't eeth' (controleer dat maar met je woordenboek). Blijft dus over dat het woord na de op één na laatste groep ;48 er uitziet als t ee. En dat kan volgens Legrand alleen maar het woord tree zijn. Daarmee heeft hij dan gevonden dat (staat voor de letter r.

In de hele tekst vervangt hij nu (door de letter r. Daarna gaat hij opnieuw kijken of er soms nog meer stukken zijn waar slechts één of twee tekens ontbreken, zodat raden van het goede woord weer een paar tekens oplevert. Die worden dan ingevuld, waarna er mogelijk weer een paar woorden geraden kunnen worden, en zo gaat dat maar door.

Werk dat zelf maar eens uit, als je daar zin in hebt.

De oplossing Hopelijk ben je er nu wel van overtuigd dat het stuk geheimschrift van Legrand met een gedegen kennis van de taal waarin de klare tekst moet komen te staan, en een slimme aanpak, niet zo moeilijk te ontcijferen is.

Oh, je wilt nog weten wat het uiteindelijke resultaat was? Nou, hier komt het:

*A good glass in the bishop's hostel in the devil's
seat fortyone degrees and thirteen minutes
northeast and by north main branch seventh limb
east side shoot from the left eye of the
death's-head a bee-line from the tree through the
shot fifty feet out!*

Of in het Nederlands:

*Een goed glas wijn in de herberg van de bisschop
in de duivelsstoel eenenveertig graden dertien
minuten noordoost ten noorden stam zevende
zijtak oostkant schiet door het linkeroog van het
doodshoofd een rechte lijn van de boom door het
schot vijftig voet verder*

Misschien denk je nu bij jezelf dat ook dáár nog geen touw aan vast te knopen is. Dat dacht Legrand eerst ook. Uiteindelijk bleek dat mee te vallen, maar daarvoor moet je het verhaal van Edgar Allan Poe zelf maar lezen.

1 DIT IS EEN GEHEIM BERICHT

2

W	I	S	K	U	N	D	E
---	---	---	---	---	---	---	---

3

D	I	T	I	S	E	E	N
G	E	H	E	I	M	B	E
R	I	C	H	T	X	X	X

4

8	3	6	4	7	5	1	2
---	---	---	---	---	---	---	---

5

1	2	3	4	5	6	7	8
EBX	NEX	IEI	IEH	EMX	THC	SIT	DGR

Bij kolomtranspositie maakt men gebruik van een sleutelwoord waarin elke letter maar één keer mag voorkomen. Hier is dat WISKUNDE (2). De klare tekst (1) wordt daar in regels met dezelfde lengte onder geschreven (3), eventueel aangevuld met een aantal letters X. De kolommen worden daarna genummerd volgens de volgorde waarin de letters van het sleutelwoord in het alfabet voorkomen (4). (Dus WISKUNDE → E D I K N S U W → 1 2 3 4 5 6 7 8.) De cijfertekst komt tot stand door de kolommen van boven naar beneden in volgorde van hun nummer achter elkaar te schrijven (5).

Voor het ontcijferen van de cijfertekst moet je over het sleutelwoord beschikken. Dan kun je in omgekeerde richting werkend de klare tekst te voorschijn toveren.

Uitdaging van Edgar Allan Poe

Zoals je hebt gezien, had Edgar Allan Poe veel belangstelling voor geheimschrift. In 1839 werkte hij mee aan 'Alexander's Weekly Messenger', een tijdschrift dat in Philadelphia werd uitgegeven. Daarin daagde hij lezers uit hem boodschappen in geheimschrift te zenden, die hij dan zou ontcijferen. Zo ontving hij van een zekere G. W. Kulp een boodschap die hij maar niet kon ontcijferen. In de mening dat hij bedrogen werd (er zou geen enkel systeem achter zitten, en die cijfertekst zou uit wat lukraak achter elkaar gezette tekens bestaan), publiceerde Poe de boodschap uiteindelijk in de Messenger.

Zo kon pas veel later worden vastgesteld dat de boodschap van Kulp versleuteld was volgens het systeem van de Vigenère.

De problemen die Poe met het ontcijferen van de boodschap had, zijn mogelijk te wijten aan het moeilijk leesbare handschrift van Kulp. Het ligt echter meer voor de hand dat Poe niet wist hoe je een vigenère moest ontcijferen, zonder enige kennis omtrent het sleutelwoord. Hoe je daaraan moest komen, zou Kasiski pas in 1860 laten zien. Maar toen leefde Poe al niet meer.

Zelf aan de slag

Tot nu toe hebben we drie methoden voor het versleutelen van een cijfertekst volledig behandeld: het caesaralfabet, de vigenère en de binaire code van Bacon.

In navolging van Edgar Allan Poe, willen we je dan ook uitdagen volgens één van deze drie methoden een cijfertekst in elkaar te zetten, en naar ons op te sturen. Vergeet niet de sleutel daarbij te voegen, want het is niet de bedoeling dat je een cijfertekst maakt, die moeilijk te ontcijferen is. Zulke doorgewinterde crypto-analysten zijn we nu ook weer niet!

Het liefst zien we een aardige cijfertekst, waaruit een leuke klare tekst te voorschijn komt. De meest originele vondsten zullen we zeker in Pythagoras opnemen.

Wanneer je die uitdaging te lastig vindt, kun je ook proberen de onderstaande cijfertekst te ontcijferen. Je inspanningen zullen zeker niet voor niets zijn!

GKXXO OBTON SDROL DYXDM STPOB NUEXT
ONQYZ VYBBS XQXKK BRODB ONKMD SOCOM
BODKB SKKDC DEBOX TONSX QDNKX WOOXK
KBOOX VOEUO FOBBK CCSXQ

Palindromen

Palindromen

Een palindroom (of keerwoord) is een woord dat bij omdraaiing van de letters hetzelfde woord oplevert. Bijvoorbeeld: pap, dood, negen, meetsysteem.

In zijn boek 'Opperlandse taal- & letterkunde' (waaruit hieronder een gedeelte) geeft Battus zo'n zeshonderd van dergelijke woorden in het Nederlands. Wanneer dit soort woorden je interesseren, moet je dat boek er maar eens op naslaan. Hier gaan we daar niet verder op in.

Want... ook in de wiskunde komen palindromen voor. Uiteraard zijn het dan geen woorden maar getallen.

22a ¹ Driehonderdendrie prachtige keerwoorden									
j	dood	sawa's	kalklak	gortrog	legvogel	topkookpot			
aha	ebbe	sexes	kapopak	klokloik	maandnaam	11			
ara	ecce	shahs	karvrak	knippink	maatraam	gardegedrag			
dod	ette	solo's	keizeik	kolkklok	Malagalam	gardegedrag			
eke	egge	stuts	keizeik	kortrok	Malavalam	legerkregel			
ene	elle	tenet	kortrok	kotstok	markikram	lekenkregel			
ere	emme	tenet	kutstok	krabstok	mezebezem	lekenkregel			
ete	enne	6	lampmal	kurkkruk	moordroom	levantnavel			
hah	eppe	eisic	lavaval	maannaam	naaldlaan	levanknevel			
hoh	esse	giffig	leiwiel	niessin	neertreën	levensnevel			
kak	geeg	gillig	martram	pitstip	Nepalapen	leverdnevel			
kek	goog	gittig	meeneem	poelloop	neppoppen	leverwnevel			
kik	kaak	kippiik	meezem	rookoor	neppuppen	lippepeppil			
kok	keek	liggil	merkem	reissier	netebeten	meetsysteem			
kijk	kook	lossol	modedom	seissies	neteneten	morgegegom			
lal	neen	neggen	nepapen	siammais	paalslaap	nedertreden			
lel	paap	nekken	netsten	sierreis	paardraap	pokkedekkop			
lil	raar	nellen	ottetto	snakkans	pergreep	staalplaats			
lol	soos	neppen	paalaap	snellens	plutotulp	strengnerts			
lul	tuut	netten	palmlap	spittips	polkaklop	taartstraat			
mam	5	nijlijin	papapap	tuittuut	poelsloop	teeltatleet			
mem	arkra	nippijn	petstep	9	portstrop	troostsoort			
mom	eikie	pikkip	pilsip	avondnova	roomsloor	12			
mum	epope	redder	pompomp	doornrood	silopolis	koortsstrook			
non	eiste	reeder	postop	draaiaard	snorfrons	kornettenrok			
oho	geleg	rekker	prodop	draagaard	spurttrups	neppikkippen			
ovo	gezeg	reller	racecar	draaiaard	stormrots	neppaatspen			
ozo	kajak	remmer	randnar	draaiaard	stortrots	partiertrap			
pap	kazak	renner	reisier	draaiaard	strafaris	rekkenrekker			
pep	lepel	repper	roodoor	draaiaard	stremerts	tuuttuuttuut			
pip	madam	rottor	rotator	droosmoord	sulcyclus	13			
pop	naman	sarras	rotator	edelsede	taalplaat	kaasredersaak			
pup	neden	serres	sagogas	faalslaaf	tarwewrat	mett			

Onder een **palindroom** verstaat men in de wiskunde een (natuurlijk) getal van tenminste twee cijfers dat niet van waarde verandert door omkering van de volgorde van de cijfers. Dus bijvoorbeeld 55 of 1234321 of 456787654, enz.

Natuurlijk zullen we je nu niet vragen om het grootste palindroom op te schrijven, want zoals je aan de hierboven gegeven voorbeelden al kunt zien, kun je ze zo groot maken als je maar wilt. We willen je echter wel op iets anders wijzen.

Omkeren en optellen

Kies een natuurlijk getal, bijvoorbeeld 128. Draai van dit getal de volgorde van de cijfers om. Je krijgt dan 821. Tel dan deze getallen bij elkaar op:

$$\begin{array}{r} 128 \\ 821 \\ \hline 949 \end{array}$$

En 949 is een palindroom!

Om te kijken of dat niet toevallig is, doen we hetzelfde nog eens met een ander getal, bijvoorbeeld 328:

$$\begin{array}{r} 328 \\ 823 \\ \hline 1151 \end{array}$$

Dat is geen palindroom, maar... nógmaals omkeren en optellen levert:

$$\begin{array}{r} 1151 \\ 1511 \\ \hline 2662 \end{array}$$

En dat is wel een palindroom.

Bij 79 (of 97) moet je dat omkeren en optellen wel zes keer herhalen, maar ook dan kom je op een palindroom uit, namelijk 44044.

We kunnen ons nu afvragen of dat proces van omkeren en optellen bij alle getallen tot een palindroom zal leiden.

Om het ons gemakkelijk te maken, zullen we dat eerst eens nagaan voor alle getallen die uit twee cijfers bestaan (dus van 10 tot en met 99).

Okee, zul je dan misschien zeggen, we proberen die gewoon allemaal uit. Tenslotte is dat aantal te overzien.

Maar zoals echte wiskundigen zouden zeggen: dat is weinig elegant. Anders gezegd: we hebben daar geen zin in, we vinden dat te veel werk.

Dus blijft ons niets anders over dan een slimmere aanpak: een zo kort mogelijk bewijs leveren voor deze veronderstelling.

Bewijs uit luiheid?

Daar gaan we dan. Stel een getal van twee cijfers voor door ab . Dan geeft a de tientallen aan en b de eenheden. Het getal kan dan ook geschreven worden als $10a + b$.

Omkering van de cijfers levert een getal dat geschreven kan worden als $10b + a$. Optellen van $10a + b$ en $10b + a$ geeft $11a + 11b$, hetgeen ook geschreven kan worden als $11(a + b)$.

Wanneer $a + b$ kleiner of gelijk is aan 9, zijn we met één stap bij een palindroom aangeland. Ga maar na. Om te zien wat er gebeurt met de andere tweecijferige getallen moeten we de gevallen

$a + b = 10, 11, 12, \dots, 18$ apart bekijken.

Als $a + b = 10$, dan is $11(a + b)$, het getal na de eerste stap, gelijk aan 110. Omkeren levert 011. Optellen van 110 en 011 geeft 121 en dat is inderdaad een palindroom.

Op dezelfde manier kun je nu de andere gevallen nagaan. Je zult dan merken dat je steeds binnen maximaal zes stappen op een palindroom uitkomt.

Alleen als $a + b$ gelijk is aan 17 (dus alleen maar voor de getallen 89 en 98), zul je pas na 24 stappen bij een palindroom uitkomen, en wel het getal

8813200023188.

Getallen met meer dan twee cijfers

Nu zou dit bewijs pas écht mooi zijn als je het gemakkelijk aan zou kunnen passen voor getallen die bestaan uit drie cijfers, vier cijfers, enz.

Dan loont het ook de moeite. Want je hoeft dan niet alle 900 getallen van drie cijfers, alle 9000 van vier cijfers, enz. apart te onderzoeken!

We hebben een poging gewaagd voor een getal dat uit drie cijfers bestaat; abc .

Dit is ook te schrijven als $100a + 10b + c$. Het omgekeerde daarvan is $100c + 10b + a$. Tel je het getal en zijn omgekeerde op, dan krijg je $101(a + c) + 20b$. Dit kan maar liefst 180 mogelijke waarden aannemen. Immers b kan 0 tot en met 9 zijn, terwijl $a + c$ alle waarden van 1 tot en met 18 kan aannemen. Als je al die mogelijkheden wilt uitproberen, ben je wel even bezig. Om maar te zwijgen van getallen met vier of meer cijfers. We kwamen er niet uit!

Biedt de computer uitkomst?

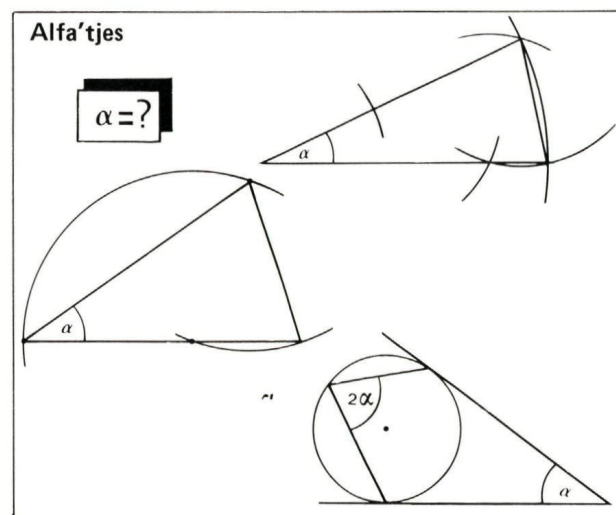
Toen bleef er niets anders meer over dan alle getallen één voor één af te gaan. Daarvoor gebruikten we natuurlijk een computer, wat dacht je!

Alle getallen tot en met 2000 zijn we afgegaan. Die kwamen allemaal op een palindroom uit. Maar ja, daarboven vind je nog oneindig veel getallen. En die zul je toch ook allemaal één voor één af moeten gaan, voordat je kunt zeggen dat *alle* getallen via omkeren en optellen tot een palindroom leiden. Dat levert uiteraard oneindig veel rekenwerk op. Zelfs als je er vanuit gaat dat elk getal dat je door de computer laat nagaan, in een beperkt aantal stappen tot een palindroom leidt.

Nu zou het prachtig zijn, als de computer tijdens dat karwei een getal tegenkomt dat niet tot een palindroom leidt. Dan zou je namelijk een tegenvoorbeeld hebben, zodat je kunt zeggen dat *niet alle* getallen via omkeren en optellen tot een palindroom leiden.

Zo'n getal geeft dan een keten van omdraaien en optellen, zonder dat het ooit een palindroom oplevert. Het gekke is dat je daar door uitproberen óók nooit achter kunt komen. Want al krijg je na tien miljoen stappen nog steeds geen palindroom, het kan altijd nog komen!

Zoals je ziet, geeft de computer geen zekerheid omtrent de uitspraak: alle getallen leiden via omkeren en optellen tot een palindroom. Het wachten is dus op een algemeen bewijs.



Een computerprogramma

Omdat de computer met de afzonderlijke cijfers van een getal moet rekenen, worden die cijfers in een rij opgeslagen. Je kunt maar het beste meteen een rij a reserveren, waar bijvoorbeeld een getal van 100 cijfers in kan worden opgeslagen, want je zult soms op behoorlijk grote getallen uitkomen. Voor het omgekeerde getal moet je een tweede rij b reserveren.

Wanneer je bijvoorbeeld het getal 7248 neemt, komen de eenheden in a (1), de tientallen in a (2), enz. Op dezelfde manier wordt het omgekeerde in de rij b opgeborgen.

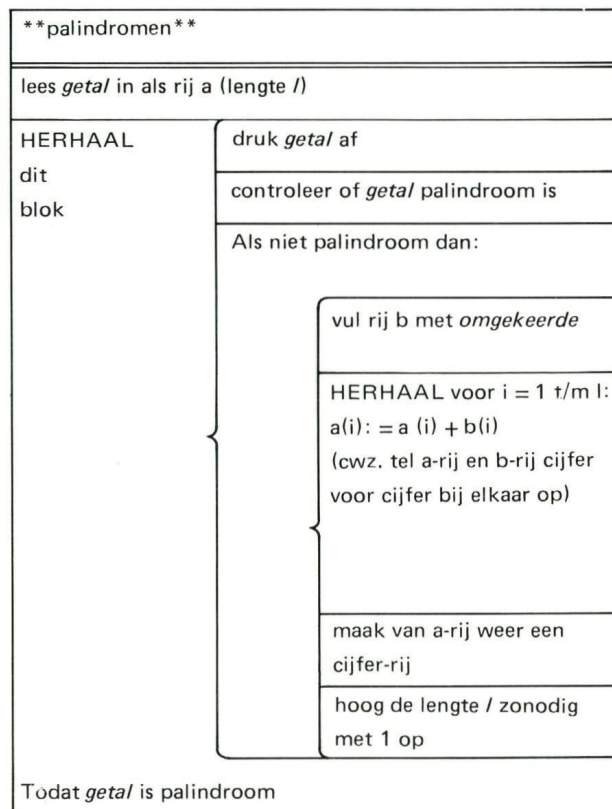
a: a(100) a(99) a(98)								a(8)	a(7)	a(6)	a(5)	a(4)	a(3)	a(2)	a(1)
0	0	0						0	0	0	0	7	2	4	8
b: b(100) b(99) b(98)								b(8)	b(7)	b(6)	b(5)	b(4)	b(3)	b(2)	b(1)
0	0	0						0	0	0	0	8	4	2	7

Het proces van 'omkeren en optellen' verloopt voor 7248 als volgt.

a-rij: ... 0 0 0 7 2 4 8 *getal* (l=4)
b-rij: ... 0 0 0 8 4 2 7 omgekeerde
a-rij: ... 0 0 1 5 6 7 5 nieuw *getal*: de som (l=5)
b-rij: ... 0 0 5 7 6 5 1 omgekeerde
a-rij: ... 0 0 7 3 3 2 6 nieuw *getal*: de som (l=5)
b-rij: ... 0 0 6 2 3 3 7 omgekeerde
a-rij: ... 0 1 3 5 6 6 3 nieuw *getal*: de som (l=6)
b-rij: ... 0 3 6 6 5 3 1 omgekeerde
a-rij: ... 0 5 0 2 1 9 4 nieuw *getal*: de som (l=6)
b-rij: ... 0 4 9 1 2 0 5 omgekeerde
a-rij: ... 0 9 9 3 3 9 9 nieuw *getal*: palindroom

De lengte l van een getal uit de a-rij heeft de computer nodig om het omgekeerde van dat getal in de b-rij te krijgen. Het optellen gaat uiteraard cijfer voor cijfer, volgens het systeem 'zoveel opschrijven, en zoveel (0 of 1) onthouden'.

Omdat er nogal wat computertalen of varianten daarvan worden gebruikt, zullen we ons weer beperken tot een **structuurdiagram**. Dat is nog lang geen programma, maar het zal je zeker een eind op weg helpen.



Als je programma af is

Wanneer je een goed werkend programma hebt, en daarmee opvallende resultaten vindt, moet je het ons maar eens laten weten!

Ook kun je dan eens kijken of je dat programma kunt gebruiken bij het oplossen van de twee volgende problemen.

Probleem 1 De getallen 121 en 484 zijn niet alleen palindromen, maar het zijn ook kwadraten (resp. van 11 en 22). Elk bestaan ze uit een oneven aantal cijfers.

Probeer het kleinste palindroom te vinden dat uit een even aantal cijfers bestaat en eveneens een kwadraat is.

Probleem 2 Zoek een getal dat uit zes cijfers bestaat, en na vermenigvuldiging met één van de getallen 2 tot en met 9, een getal levert dat uit dezelfde zes cijfers bestaat, maar nu in omgekeerde volgorde.

Leibniz' nieuwe methode

Als je kunt differentiëren, zul je de nu volgende beschrijving van de 'nieuwe methode' misschien wat flauw vinden. Maar probeer jezelf eens in een 17e eeuwse wiskundige te verplaatsen, die nog niet meer weet dan dat een vergelijking in x en y een kromme voorstelt, en die alle onderzoeken over raaklijnen van nabij volgt. Wie praat er dan nog over flauw?

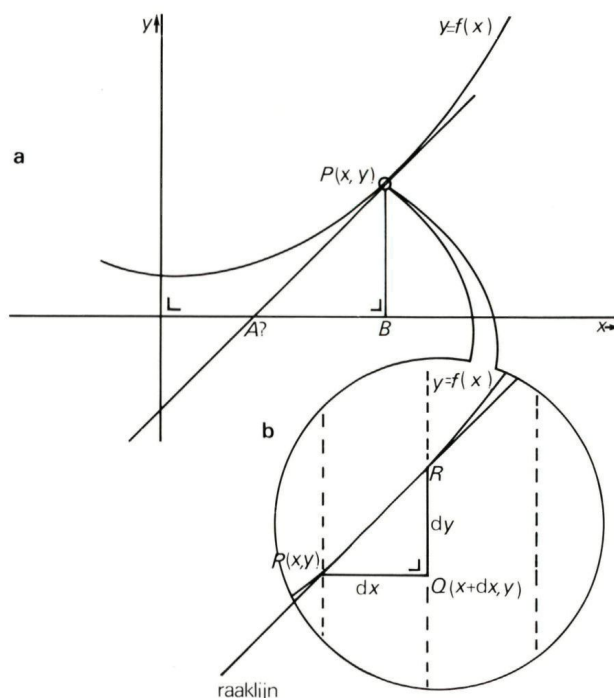
Een raadselachtig stuk wiskunde

De 'nieuwe methode' was voor de tijdgenoten van Leibniz een raadselachtig stuk wiskunde. Want Leibniz wilde in het uiteindelijk in 1684 verschenen artikel geen gebruik maken van oneindig kleine getallen. Waarschijnlijk verwachtte hij daar fel verzet tegen. Hierdoor heeft de 'nieuwe methode' iets magisch: je kunt hem gebruiken om vergelijkingen van raaklijnen te bepalen, waarom hij werkt blijft echter verborgen. Maar gelukkig brengen de bewaard gebleven aantekeningen van Leibniz uit de periode 1675–79 een stuk duidelijkheid. Daar is namelijk uit op te maken hoe hij, gebruikmakend van oneindig kleine getallen, zijn methode gevonden heeft.

Voor de duidelijkheid draaien wij hier de zaken om. Eerst bespreken we de aantekeningen van Leibniz, en daarna laten we in het kort zien, waar het artikel uit 1684 daarvan afweek.

Leibniz' aantekeningen

Op de grafiek van een of andere functie f ligt een punt $P(x, y)$. Leibniz zoekt nu de vergelijking van de raaklijn in het punt P aan de grafiek. Daartoe berekent hij eerst de coördinaten van A , het snijpunt van de raaklijn met de x -as (zie figuur a hiernaast, waarin ook nog het punt $B(x, 0)$ getekend is). Daarbij doet hij net of de grafiek bestaat uit *oneindig veel oneindig kleine lijnstukjes*. Het verschil tussen de x -coördinaten van twee opeenvolgende punten van de grafiek (zoals P en R in figuur b, een stukje van de grafiek in de omgeving van P dat onder de microscoop sterk uitvergroot is) wordt door Leibniz constant genomen. Hij noemt dit verschil dx (d van het Latijnse differen-



tia, verschil). De raaklijn in P is dan voor hem eenvoudig de lijn die tussen P en R met de grafiek van f samenvalt.

In figuur b is die raaklijn PR getekend. Bovendien is daarin ook $\triangle PQR$ aangegeven, met Q het punt $(x + dx, y)$.

Deze $\triangle PQR$ is gelijkvormig met $\triangle ABP$ uit figuur a. Immers PQ is evenwijdig met AB , RQ met PB , en PR is de raaklijn die dus ook door A gaat. Uit deze gelijkvormigheid volgt:

$$\frac{RQ}{PQ} = \frac{PB}{AB}$$

Hierin is $PQ = dx$. RQ wordt door Leibniz dy genoemd, en $PB = y$ is gegeven, zodat er komt te staan:

$$\frac{dy}{dx} = \frac{y}{AB}$$

Hieruit is AB te vinden, als je de verhouding $\frac{dy}{dx}$ kunt

berekenen. En voor die berekening leidt Leibniz een serie regels af (*een opmerkelijk soort rekenmechanisme*).

1 a constant geeft $da = 0$!

2 a constant geeft $d(ax) = a \cdot dx$

Als dx het verschil in x is, dan is het verschil in ax : $d(ax) = a(x + dx) - ax = dx$.

$$3 \quad d(x+y) = dx + dy \text{ en } d(x-y) = dx - dy$$

Als dx het verschil is in x , en dy het verschil in y , dan is het verschil in $x+y$:

$$d(x+y) = \{(x+dx) + (y+dy)\} - (x+y) = dx + dy.$$

$$4 \quad d(xy) = xdy + ydx$$

Het verschil in xy is:

$$d(xy) = \{(x+dx) \cdot (y+dy)\} - xy = xdy + ydx + dx \cdot dy, \text{ maar } dx \cdot dy \text{ is het produkt van twee oneindig kleine getallen, dat te verwaarlozen is ten opzichte van } xdy + ydx.$$

Als je in regel 4 x invult voor y , vind je:

$$d(x \cdot x) = xdx + xdx, \text{ dus } d(x^2) = 2xdx.$$

De volgende stap is $d(x^3) = d(x \cdot x^2) =$

$$xd(x^2) + x^2dx = x \cdot 2xdx + x^2dx = 3x^2dx.$$

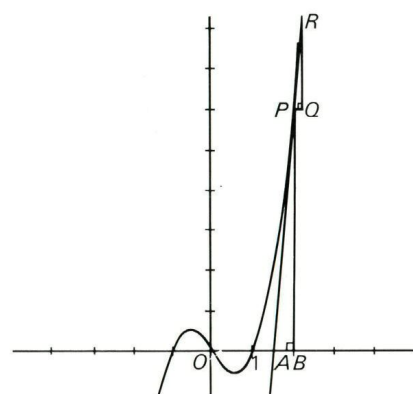
Zo komt Leibniz tot:

$$5 \quad d(x^n) = nx^{n-1}dx$$

Tenslotte leidt hij voor $d(\frac{x}{y})$ af:

$$6 \quad d(\frac{x}{y}) = \frac{ydx - xdy}{y^2}$$

Voorbeeld Neem nu eens de functie $f(x) = x^3 - x$, waarin de raaklijn in $P(2,6)$ bepaald moet worden.



Grafiek van $f(x) = x^3 - x$ met de raaklijn in $P(2,6)$

$$\text{Nu is: } \frac{dy}{dx} = \frac{PB}{AB} = \frac{6}{AB}.$$

Maar $y = x^3 - x$, dus volgens de regels 3 en 4 geldt voor dy :

$$dy = d(x^3 - x) = d(x^3) - dx = 3x^2dx - dx = (3x^2 - 1)dx = 11dx \text{ (want } x = 2).$$

Dit levert dan:

$$\frac{dy}{dx} = \frac{11dx}{dx} = 11,$$

zodat $11 = 6/AB$, ofwel $AB = 6/11$. B is bekend, waardoor je voor A het punt $(16/11, 0)$ vindt. De raaklijn is dus de lijn door $(16/11, 0)$ en $(2, 6)$. En daarmee kun je de vergelijking ervan opstellen.

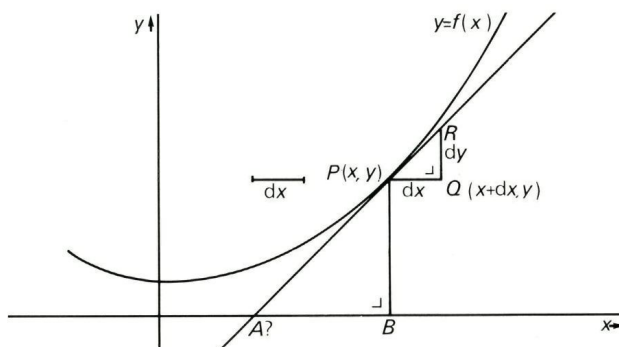
Maxima en minima, zegt Leibniz, zijn er als $dy = 0$ (PR moet evenwijdig zijn aan de x -as). In dit voorbeeld is dat het geval voor $x = \pm \frac{1}{3} \sqrt{3}$. Ga maar na!

Afwijkingen in het artikel

Waarin wijkt het uiteindelijke artikel uit 1684 nu af van Leibniz' aantekeningen?

Leibniz stelt in zijn artikel dezelfde vraag als hierboven: wat is de vergelijking van de raaklijn in $P(x, y)$ aan de grafiek van de functie f ?

Nu neemt hij een willekeurig *eindig* lijnstuk, en noemt de lengte daarvan dx (zie onderstaande figuur). Punt Q heeft dan coördinaten $(x+dx, y)$, en voor R neemt Leibniz *op de raaklijn* het punt met x -coördinaat $x+dx$. R ligt dus niet meer zoals in de aantekeningen, op de grafiek. QR wordt weer aangegeven met dy .



$\triangle PQR$ is nu een driehoek met eindige afmetingen geworden, maar nog steeds geldt:

$$\frac{dy}{dx} = \frac{y}{AB}.$$

En dan komt het konijn uit de hoge hoed, want voor de berekening van de verhouding van de *eindige* lijnstukken dy en dx geeft Leibniz zonder enig bewijs dezelfde regels 1 tot en met 6 die hij ook in zijn aantekeningen met *oneindig kleine* lijnstukjes had afgeleid. De lezer moest maar raden waar die regels vandaan kwamen. Maar — wonder boven wonder — de 'nieuwe methode' bleek uitstekend te werken.

Pythagoras Olympiade



Nieuwe opgaven (Oplossingen inzenden vóór 1 januari 1985 aan *Pythagoras Olympiade, Cornelis Krusemanstraat 60II, 1075 NS Amsterdam (NL)*. Wedstrijdvoorwaarden en prijzen staan vermeld op pagina 8 van dit nummer.)

PO 70

Een commissie telt 15 leden: 6 uit Den Haag, 2 uit Gouda en 7 uit Arnhem.

1. In welke plaats aan de weg Den Haag–Arnhem, moet de commissie vergaderen om de totale reiskosten zo laag mogelijk te houden?

2. En als de commissie wordt uitgebreid met nog twee leden uit Arnhem?

We vragen gemotiveerde antwoorden; je mag aannemen dat de reiskosten evenredig zijn met de af te leggen afstand.

PO 71

Bewijs dat de kans dat Nieuwjaarsdag op zondag valt *niet* precies gelijk is aan $1/7$. (In ons kalendersysteem zijn 2000, 2400, 2800, ... wél schrikkeljaren, maar de andere eeuwen zoals 1900, 2100, 2200, ... niet!)

PO 72

Op een bord zitten 16 lampjes gerangschikt in een cirkel. Elk lampje kun je met een schakelaartje aan of uit zetten. Bovendien is er een rode knop waarmee je de toestand van alle lampjes tegelijk kunt beïnvloeden. De nieuwe toestand van elk lampje hangt daarbij uitsluitend af van de toestand van dat lampje en z'n rechterbuurlamp vóór het drukken. Namelijk als L zo'n lampje is, dan geldt:

- waren L en z'n buurman beide aan, of beide uit, dan gaat (of blijft) L aan;
- was één van beide aan, en de ander uit, dan gaat (of blijft) L uit.

Bewijs dat alle lampjes branden als je, uitgaande van een willekeurige begintoestand, 16 keer achter elkaar op de rode knop hebt gedrukt.

Oplossingen en prijswinnaars van de opgaven

PO 56–60

PO 56

Iemand wil tien vierkanten van gelijke afmetingen in een vlak tekenen zonder dat ze elkaar overlappen, maar zo, dat één van die vierkanten de negen andere raakt. Bewijs dat dit onmogelijk is.

Oplossing van *Jan de Boer*, 5 vwo, RSG Magister Alvinus, Sneek:

Stel dat de vierkanten zijde 1 hebben. Neem een vierkant, en teken er omheen een vierkant met zijde 2 (netjes symmetrisch: het grote ontstaat uit het kleine door puntvermenigvuldiging vanuit het centrum met een factor 2). Een eenheidsvierkant dat het kleine vierkant raakt, snijdt van de zijden van het grote vierkant een zeker stuk s af. De bewering is dat in *alle* mogelijke gevallen geldt dat de lengte van s minstens 1 is. Jan heeft dit netjes uitgewerkt, en daarbij zes mogelijke gevallen onderscheiden. Ruimtegebrek verhindert ons dat allemaal hier over te nemen.

De omtrek van het grote vierkant is 8, en volgens het bovenstaande is er dus om het kleine vierkant maar plaats voor ten hoogste 8 rakende vierkanten.

Er waren 18 inzendingen, maar slechts 4 ervan waren correct: *Jan de Boer*, *Menke Ubbens* 5 vwo, RSG Magister Alvinus, Sneek, *Rutger Noot*, 6 g, Gymnasium Haganum, Den Haag, en *Auke Zijlstra*, 6 ath, RSG Leeuwarden. De prijzen gingen naar Jan en Menke.

PO 57

Suzie Slim heeft een kwis gewonnen. Als beloning krijgt ze honderd genummerde pionnen die ze op de hoekpunten van een regelmatige honderdhoek moet plaatsen. Ze verdient dan voor elk van de honderd zijden een bedrag in centen dat gelijk is aan het produkt van de nummers van de twee pionnen die op de aangrenzende hoekpunten staan.

Zou ze de pionnen gewoon op volgorde zetten, dan zou ze dus $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + 99 \cdot 100 + 100 \cdot 1$

centen krijgen. Maar ze hoeft ze niet in deze volgorde te plaatsen. Hoe moet Suzie de pionnen zetten om zo veel mogelijk geld in de wacht te slepen?

Oplossing van *Rutger Noot*, 6 g, Gymnasium Haganum, Den Haag, en *Menke Ubbens*, 5 vwo, RSG Magister Alvinus, Sneek: Nummer de hoekpunten opvolgend 1 t.e.m. 100. Het nummer van de pion op hoekpunt a noemen we n_a . Als we de volgorde van de pionnen op het traject van a naar b omdraaien, verandert alleen de opbrengst van de twee verbroken schakels. Die opbrengst was $n_{a-1}n_a + n_b n_{b+1}$, en na de omdraaiing is het $n_{a-1}n_b + n_a n_{b+1}$. Zo'n verandering is dus gunstig als $n_{a-1}n_b + n_a n_{b+1} - n_{a-1}n_a - n_b n_{b+1} = (n_{a-1} - n_{b+1})(n_b - n_a) > 0$ is.

Begin nu met een willekeurige verdeling. We kunnen veronderstellen dat de pion met nummer 1 op hoekpunt 1 staat. Als pion 2 nu niet op hoek 2 of hoek 100 staat, is verwisseling van het traject van hoek 2 t.e.m. de hoek waar pion 2 staat, gunstig; staat pion 2 op nummer 100, dan maakt verwisseling van de pionnen op het traject 2, 3, ..., 100 niets uit. We kunnen dus aannemen dat pion 1 op hoek 1 staat en pion 2 op hoek 2. Als pion 3 niet op hoek 100 staat, is de verwisseling van het traject tussen pion 3 en hoek 100 gunstig.

Daarna hebben we dus pion 1 op 1, pion 2 op 2 en pion 3 op 100. Zo doorgaand kunnen we laten zien dat we telkens méér krijgen door ervoor te zorgen dat pion 4 op 3 komt, pion 5 op 99, pion 6 op 4, pion 7 op 98, enzovoorts. De maximale opbrengst voor Suzie is dus $1 \cdot 2 + 1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + 5 \cdot 7 + \dots + 89 \cdot 100 + 99 \cdot 100 = 338153$ cent.

hoek		97	98	99	100	1	2	3	4	5.....	
pion:		9	7	5	3	1	2	4	6	8.....	

Er waren 26 inzendingen, maar alleen de inzendingen van Rutger en Menke waren foutloos. Zij krijgen dus ook de prijzen. Veel inzenders vonden wel de goede volgorde, maar hun bewijzen waren niet vlekkeloos. Het is bijvoorbeeld niet voldoende als je laat zien dat elke verwisseling vanuit de 'optimale' stand een lagere opbrengst geeft. Het zou immers best kunnen dat je na een aantal verwisselingen toch weer hoger gaat uitkomen.

PO 58

Is het mogelijk dat velden van een schaakbord zo te nummeren van 1 tot en met 64 dat de nummers van twee velden die een zijde of een hoekpunt gemeen hebben altijd hoogstens 8 verschillen?

Geef zo'n nummering, of een bewijs dat het niet kan.

Oplossing van *Pim van Hove*, 5 ath, Thijcollege, Oldenzaal: De grootst mogelijke afstand tussen twee velden is zeven stappen (recht of schuin). Per stap kan hoogstens een verschil van 8 worden overbrugd. Totaal kan dus hoogstens $8 \cdot 7 = 56$ worden overbrugd. Het verschil tussen bijv. de velden met de nummers 1 en 64 kan dus niet overbrugd worden. Daarom is een nummering die aan de gestelde eisen voldoet onmogelijk.

Er waren 32 inzendingen, waarvan 29 correct. Prijswinnaars: *Alex Maassen v. d. Brink*, 4 vwo, SG Hugo Grotius, Delft, *Danny ten Haaf*, 4 g, Dominicus College, Nijmegen, *Frank Robijn* (6 g, RSG Koning Willem II, Tilburg) generaliseerde de opgave voor een $n \times n$ -bord.

PO 59

Bewijs dat je uit elk tiental opvolgende natuurlijke getallen er minstens één kunt kiezen dat met geen van de andere een gemeenschappelijke deler (groter dan 1) heeft. Voorbeeld: van de getallen 840 t.e.m. 849 heeft 841 = $29 \cdot 29$ geen gemeenschappelijke deler met een van de andere getallen.

Oplossing van *Hans le Grand*, 6 g, SG Bataafse Kamp, Hengelo (O):

Als we uit een serie van 10 opvolgende getallen alle getallen wegstrepen die een factor gemeen hebben met een ander getal uit die serie, dan zullen we hoogstens wegstrepen:

5 even getallen (van die tien getallen zijn er vijf even), daarna nog

2 drievouden (er zijn hoogstens vier drievouden, maar twee ervan hebben we al weggestreept omdat ze even zijn), daarna nog

1 vijfvoud (van de twee opeenvolgende vijfvouden is er één even), en

1 zevenvoud (van de maximaal twee zevenvouden is er maar één oneven).

De vier-, zes-, acht-, negen- en tienvouden zijn daarmee ook weggestreept. In een serie van 10 opvolgende getallen kunnen nooit twee tien-, elf- of hoger-vouden voorkomen. Er worden hoogstens 9 getallen weggestreept, en er blijft er dus minstens één over die geen gemeenschappelijke deler heeft met de andere getallen van de serie.

Er waren 29 inzendingen, waarvan 26 correct. Prijswinnaars: *Elke Laarhuis*, 5 ath, SG Bataafse Kamp, Hengelo (O), *Jan Bruin*, 6 g, Murmellius Gymnasium, Alkmaar.

PO 60

Gegeven is een willekeurige niet-gelijkzijdige driehoek met zijden van lengte a , b en c cm. Bewijs dat $(a + b - c)(a - b + c)(-a + b + c) < a \cdot b \cdot c$.

Oplossing van *Frank Robijn*, 6 g, RSG Koning Willem II, Tilburg:

Alle termen in rechterlid en linkerlid zijn positief (driehoeksongelijkheid). De gezochte ongelijkheid is dus gelijkwaardig met

$$(a + b - c)^2 (a - b + c)^2 (-a + b + c)^2 < a^2 b^2 c^2, \text{ dwz.}$$

$$(a + (b - c))(a - (b - c)) \cdot (b + (c - a))(b - (c - a)) \cdot$$

$$(c + (a - b))(c - (a - b)) < a^2 b^2 c^2, \text{ dwz.}$$

$$(a^2 - (b - c)^2) \cdot (b^2 - (c - a)^2) \cdot (c^2 - (a - b)^2) < a^2 b^2 c^2.$$

De driehoeksongelijkheid impliceert dat $(b - c)^2$, $(c - a)^2$ en $(a - b)^2$ kleiner zijn dan resp. a^2 , b^2 en c^2 , en omdat de driehoek niet gelijkzijdig is, zijn er ook minstens twee ongelijk aan nul. De ongelijkheid is daarmee bewezen.

Er waren 24 inzendingen, waarvan 19 correct. Prijswinnaars: *Peter v.d. Pol*, 5 vwo, Thorbecke SG, Arnhem, *Hans le Grand*, 6 g, SG Bataafse Kamp, Hengelo (O).

Jan de Boer en *Menke Ubbens* (beiden 6 vwo, RSG Magister Alvinus, Sneek) merkten op dat de ongelijkheid voor willekeurige positieve a , b en c geldig is (mits ze niet alle drie gelijk zijn). Het gegeven dat a , b en c zijden van een driehoek zijn, is dus overbodig. Zij gaven andere bewijzen.

Teveel of tekort?

Onderstaande vierkant-puzzel is géén gewone legpuzzel. Raakt er namelijk één klein vierkantje zoek, dan kun je van de overgebleven stukken weer hetzelfde vierkant leggen!

“Gelukkig, er bestaat tenminste iets dat onmogelijk is,” zijn we geneigd te zeggen.
Of denk jij daar anders over?

