Pythagoras

wiskunde tijdschrift voor jongeren

stichting ivio

jaargang 29
nummer 2
november 1989

Je knip op een magneetstrip

Je knip op een chip, dat zal voor het einde van dit jaar écht opgaan voor zo'n vijftienduizend inwoners van het stadje Woerden. In het kader van een Europees proefproject kunnen zij dan hun aankopen betalen met een zogenaamde chipkaart. Dat is een betaalkaart die is voorzien van een echte chip. Elektronisch betalen, zoals dat wordt genoemd, met de chipkaart is stukken betrouwbaarder dan met de magneetstripkaart die op het ogenblik uitgebreid zijn intrede doet. Bovendien kan de chipkaart nog heel wat meer dan alleen maar betalen.
In het artikel 'Zero knowledge proofs' worden de chipkaart en de werking daarvan uitvoerig beschreven. De wiskundige achtergrond er van komt aan bod in het artikel 'Modulair worteltrekken'. In dit stukje wordt het systeem rond de magneetstripkaart in het kort beschreven.

Magneetstripkaart
De zogenaamde magneetstripkaart is een gewone giro- of bankpas (figuur 1) met aan de achterzijde een zwarte magneetstrip (figuur 2). Op die magneetstrip kan net als bij een muziekcassette informatie worden vastgelegd. Niet veel, ongeveer honderd tekens. Net genoeg dus voor bij voorbeeld de naam van de eigenaar of eigenaresse, zijn of haar bank- respectievelijk gironummer en het nummer van de pas.
Bij deze pas hoort een geheime code, een getal van slechts vier cijfers. Dit is de zogenaamde PIN-code (PIN is de afkorting van Persoonlijk Identificatie Nummer). De Pin-code staat *niet* op de magneetstrip! Het is de bedoeling dat houders en houdsters van de kaart hun PIN-code geheim houden en alleen maar intoetsen als ze de pas gebruiken om te betalen of om geld op te nemen.

Unieke combinatie
Waarom bestaat de PIN-code uit maar vier cijfers? Met vier cijfers kun je maar 9999 verschillende getallen maken, als je 0000 niet

Figuur 1. Voorzijde van een magneetstripkaart. In dit geval de giromaatpas van de Postbank.

Figuur 2. Achterzijde van de giromaatpas. De donkere balk boven is de magneetstrip.

Figuur 3. Geld opnemen uit een automaat. Hier een zogenaamde Giromaat van de Postbank.

meetelt. Natuurlijk zijn er veel meer dan 9999 rekeninghouders met een pas plus PIN-code. Kortom, er zullen heel wat pas-eigenaren zijn met dezelfde PIN-code. Dat is niet erg, want de PIN-code is slechts een aanvulling op de gegevens die op de magneetstrip van de pas staan. Samen met deze gegevens vormt de PIN-code een *unieke* combinatie. De PIN-code zorgt als het ware voor een koppeling tussen kaart en rechtmatige eigenaar.

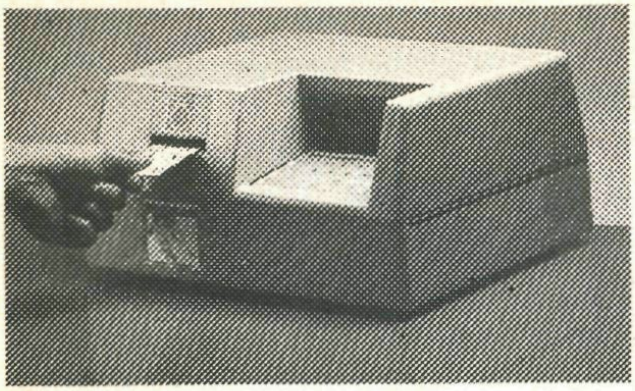
Geld opnemen

Met de magneetstripkaart kun je geld uit een automaat (figuur 3) opnemen. Hoe dat gaat zal zo langzamerhand iedereen wel weten. Je stopt je magneetstripkaart in de automaat, tikt je PIN-code in en na enkele ogenblikken krijg je het gevraagde bedrag.

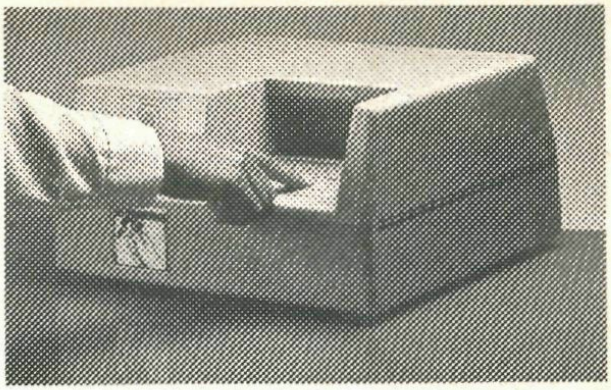
De werking is in grote lijnen vrij eenvoudig. De automaat staat in verbinding met de centrale computer van de bank. De automaat leest de gegevens van de magneetstrip af en zendt die samen met de ontvangen PIN-code naar de centrale computer. Die gaat na of de combinatie van strip-gegevens en PIN-code klopt en of het saldo van de betreffende rekening toereikend is. Is aan alles voldaan, dan krijgt de automaat van de centrale computer het sein om uit te betalen.
Neem je geld op bij het loket van een postkantoor of van een bank, dan gebeurt in wezen hetzelfde. Je geeft je pas af aan de loketbediende, deze stopt hem in een apparaatje dat de gegevens van de strip leest en je tikt je PIN-code in op een kastje naast het loket. Alles gaat weer naar de centrale computer en na akkoord bevinding kan de bediende je het gewenste bedrag uitbetalen.

Betalen

Betalen gaat op dezelfde manier als geld opnemen. In de winkel



Figuur 4. De kaart gaat in de betaalautomaat die in de winkel staat.



Figuur 5. Het intikken van de PIN-code bij een betaalautomaat.

waar je iets hebt gekocht, staat een kastje. Daar steek je de magneetstripkaart in (figuur 4) en de gegevens van de strip worden weer gelezen. Vervolgens tik je de PIN-code en het te betalen bedrag in (figuur 5). Strip-gegevens, PIN-code en te betalen bedrag gaan weer naar de centrale computer, die alles keurig controleert en vervolgens akkoord verklaart.

Nadeel

Uit een oogpunt van veiligheid moeten alle betaal- en geldopnameautomaten verbonden zijn met de centrale computer van de bank. Bovendien moeten de centrale computers van verschillende banken (zoals die van de Postbank, de ABN, de AMRO, de NMB, enzovoort) natuurlijk ook weer met elkaar verbonden zijn. Zo niet dan is afdoende controle van de unieke combinatie van strip-gegevens en PIN-code niet mogelijk.

Om als winkelier aan het systeem mee te kunnen doen, heb je dus naast de kosten voor de aanschaf van de apparatuur, de kosten voor de nodige verbindingen. Zeg maar de gesprekskosten. En die

Nieuwe truc met pincode dupeert velen

Van onze verslaggever

GRONINGEN — De politie krijgt de laatste tijd steeds vaker te maken met een nieuwe truc, waarmee de pincode van gestolen giromaatpasjes wordt gebroken.

De dieven gaan heel eenvoudig te werk: ze bellen de eigenaars van de pasjes en girobetaalkaarten op met de smoes dat ze de code moeten weten omdat anders de aangifte niet is af te handelen. In goed vertrouwen wordt de code gegeven, waarna enkele dagen later forse bedragen van de girorekening van de gedupeerde worden afgeschreven. De Groningse gemeentepolitie heeft de afgelopen weken met naar schatting twintig tot dertig van dergelijke gevallen te maken gekregen.

De Volkskrant, januari 1989.

kunnen bij uitgebreid gebruik van het systeem behoorlijk oplopen.

Veiligheid
In principe lijkt er niets aan de hand. Het systeem ziet er veilig uit. Immers bij verlies of diefstal van een magneetstripkaart kan een kwaadwillende vinder of dief er niets mee beginnen. Omdat hij de PIN-code niet weet, kan hij de gegevens van de strip niet aanvullen tot de voor iedere handeling gevraagde unieke combinatie.

Op goed geluk een PIN-code proberen is mogelijk. Drie keer een kans van zeg maar 1 op de 10 000, want de apparatuur staat maar drie verkeerde pogingen toe. Het lijkt dus zo goed als uitgesloten dat iemand toevallig de juiste PIN-code kiest. Vandaar dat wel andere methoden worden beproefd (zie bijgaande krantebe-richten).
Bovendien is het voor iemand die dat per se wil, niet al te ingewikkeld om een magneetstripkaart na te maken of zelfs 'lege' kaarten te kopen. Om aan echte stripgegevens te komen, zou je je kunnen indenken dat aan een betaalkastje in een winkel apparatuur worden gekoppeld. Zo gaan de stripgegevens van een betalende klant niet alleen naar de centrale computer, maar worden ze ook op een lege

Pincode-truc werkt door „knulligheid" eigenaars

Van onze verslaggever

AMSTERDAM — De door de Groningse politie gesignaleerde nieuwe truc met de pincode van gestolen giromaatpasjes blijkt uitsluitend te werken dankzij de onzorgvuldigheid of wellicht onwetendheid van sommige rekeninghouders. Enkele tientallen eigenaars lieten zich op knullige wijze de geheime pincode ontfutselen voordat zij de diefstal van het pasje hadden gemeld bij de Postbank. Daardoor konden de onverlaten in korte tijd flinke bedragen opnemen via de geldautomaat of met behulp van de eveneens gestolen girobetaalkaarten.

Volgens de Groningse politie gaan de dieven brutaal te werk. Pasje en betaalkaarten zitten meestal in tasje of portefeuille, waarin doorgaans ook gegevens over het adres van de eigenaar zijn te vinden. Enkele uren na de diefstal belt de dief de gedupeerde. Hij stelt zich voor als politie-ambtenaar of als iemand van de postale recherche, deelt mee dat aangifte van diefstal is gedaan, maar dat de zaak niet kan worden afgewikkeld omdat de pincode nog niet is genoteerd. De gedupeerde heeft dan in negen van de tien gevallen inderdaad al aangifte bij de politie gedaan en noemt argeloos zijn pincode.

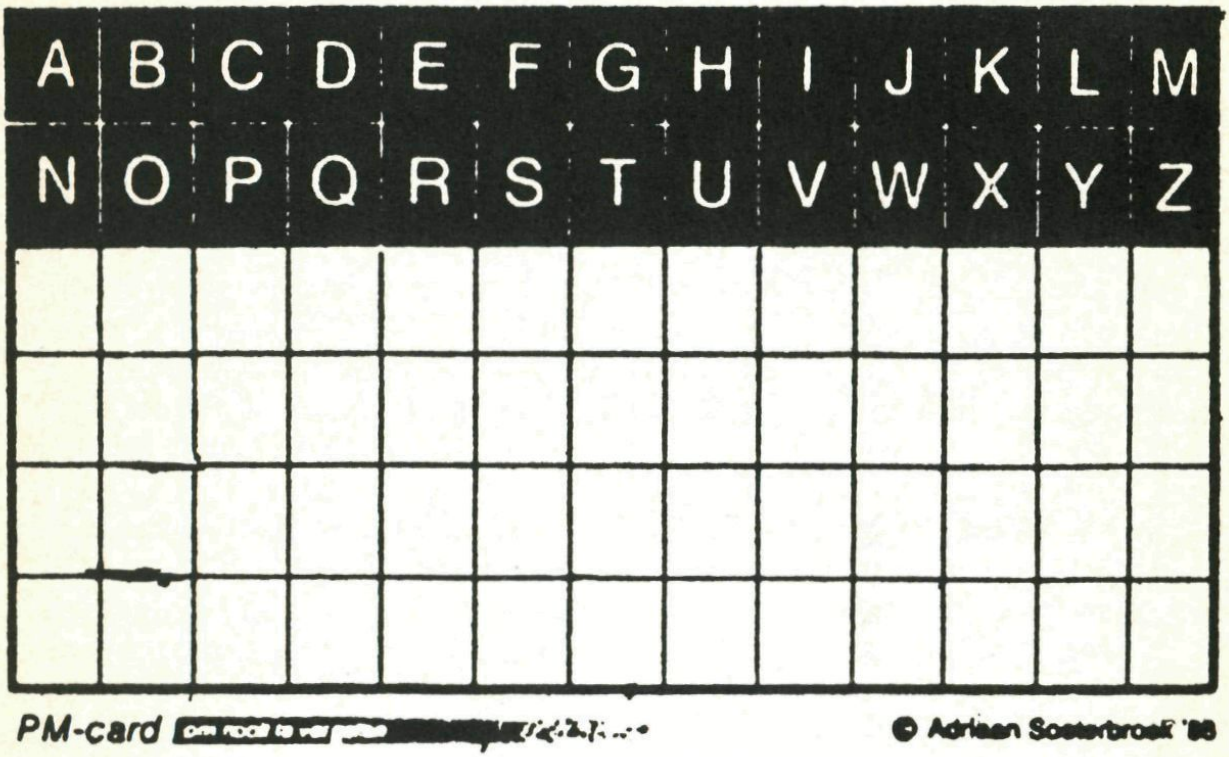
In enkele tientallen gevallen kon de dief vervolgens zonder problemen geld opnemen bij het loket of uit een geldautomaat, omdat de rekeninghouder nog geen melding van de diefstal had gedaan bij de Postbank. In feite is het plunderen van de rekening te wijten aan onwetendheid of onzorgvuldig gedrag van de rekeninghouder.

De Volkskrant, 17 januari 1989.

stripkaart gekopiëerd. Tikt de klant z'n PIN-code in, dan wordt die óók geregistreerd. Vervolgens kan met de nagemaakte kaart en de bijbehorende geregistreerde PIN-code geld op worden genomen bij een automaat.

Zo eenvoudig als het hier is beschreven, is het natuurlijk niet helemaal. Maar deze manier van oplichten is uitvoerbaar, zoals in het begin van dit jaar uitgebreid op de televisie werd gedemonstreerd. □

PIN-code onthouden



Pro-memoriekaartje

Uitvinder Soeterbroek heeft een kaartje ontwikkeld waarbij in de bovenste twee rijen de cijfers van het alfabet zijn ondergebracht. Daaronder staan vier rijen met lege hokjes.

Iemand die als PIN-code bijvoorbeeld 5638 heeft gekregen, maar dit niet denkt te kunnen onthouden — in tegenstelling tot bijvoorbeeld het woord „boot" — vult in de eerste rij onder de b het cijfer 5 in. Op de tweede rij en derde rij volgen onder de letter o de cijfers 6 en 3 en op de vierde rij onder de letter t het cijfer 8.

De andere vakjes moet de rekeninghouder opvullen met willekeurige cijfers.

Soeterbroek heeft uitgerekend dat er 1.180.000 mogelijkheden zijn. „Het is ook veel gemakkelijker om op de gok vier cijfers in te drukken, want dan heeft men een kans van 1 op 9999 op een goede oplossing."

(de Volkskrant van 20 september)

Zero knowledge proofs

Je knip op een chip

Hoe kun je bewijzen dat je iets weet of kent — een bewijs van een stelling, het antwoord op een quizvraag, een PIN-code of een computer password — zonder dat je van die kennis ook maar het geringste deel prijsgeeft? Met andere woorden, hoe kun je iemand ervan overtuigen dat je over bepaalde informatie beschikt zonder die informatie zelf te onthullen? Dat lijkt een onmogelijke, ja zelfs absurde opgave. Toch is dit precies wat moderne wiskundige technieken mogelijk hebben gemaakt. We zullen de principes ervan uitleggen.

Anton en Vera

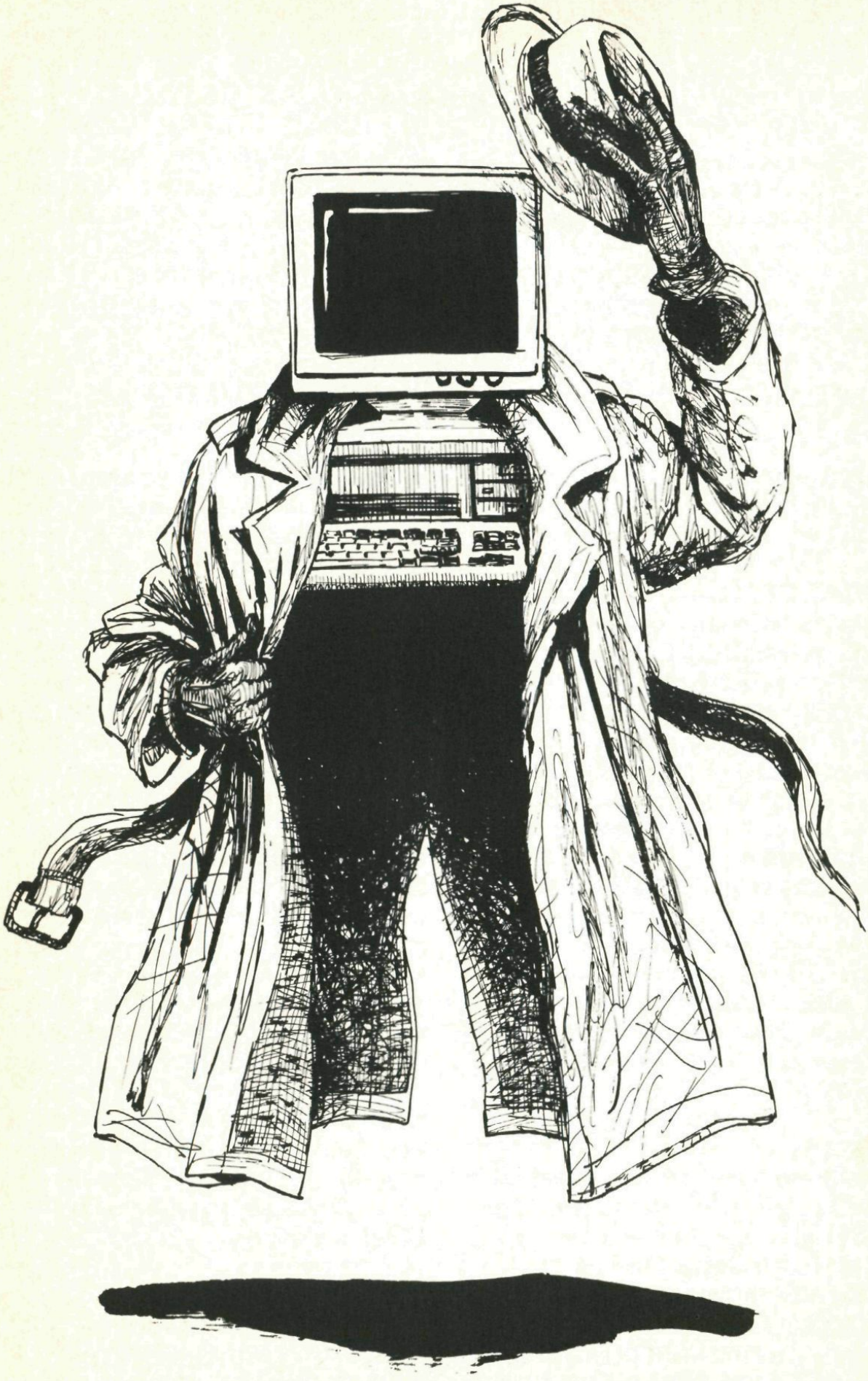
Het komt er op neer dat er een soort vraag-en-antwoordspel gespeeld wordt tussen degene die wil *aantonen* dat hij iets weet — laten we hem Anton noemen — en een kritische ondervraagster die we Vera gedoopt hebben. Na afloop van het vraaggesprek is Vera ervan overtuigd dat Anton inderdaad weet wat hij zegt te weten, maar zelf is ze geen steek wijzer geworden.
De toepassingsmogelijkheden zijn legio. Bij voorbeeld overal waar op de een of andere vorm wachtwoorden gebruikt worden. Gecombineerd met de moderne chipkaart-technologie maken die methodes ook betaalpasjes en paspoorten mogelijk die niet vervalst kunnen worden.

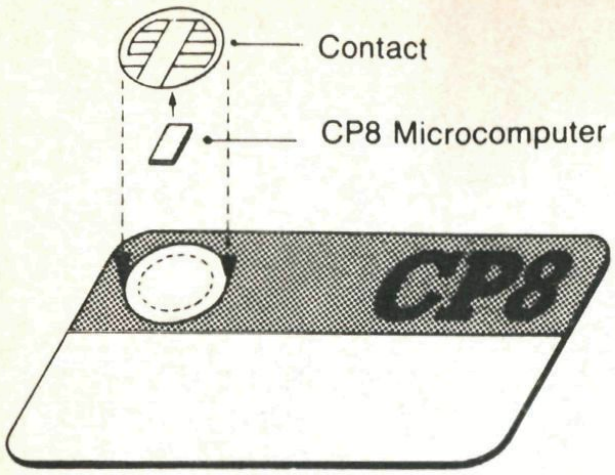
Ontbinden

Alles berust er op dat bepaalde wiskundige problemen weliswaar in theorie oplosbaar zijn, maar in de praktijk onoverkomelijke moeilijkheden geven omdat hun oplossing zelfs met de krachtigste supercomputers letterlijk eeuwen rekentijd vergt. Zo'n vraagstuk is bij voorbeeld het ontbinden in factoren van grote getallen.
Neem twee grote priemgetallen P en Q van ongeveer honderd cijfers elk. Met moderne technieken is het betrekkelijk eenvoudig om zulke grote priemgetallen te vinden. Bepaal hun produkt $M = P \cdot Q$. Ook dat is niet moeilijk; het resultaat is een getal van ongeveer 200 cijfers.
Het getal M maak je bekend, maar P en Q houd je geheim. Een ander zal er dan nooit in slagen om die ontbinding van M terug te vinden. De snelste ontbindingstechnieken die er op dit moment bekend zijn, kosten namelijk zelfs met de grootste computers voor zulke grote getallen letterlijk eeuwen computertijd.

Chipkaart

Voordat we beginnen aan de uitleg van die zogenaamde *zero knowledge proofs* (bewijzen waarbij geen kennis wordt overgedragen) eerst iets over de chipkaart. Dat is een klein technisch wonder. Een goudkleurig schijfje ter grootte van een kwartje zit ingebakken in een plastic kaart met





De chipkaart.

het formaat van een betaalpas. Het gouden schijfje bevat een chip waarin zich bij voorbeeld een 8-bits microcomputer, een 128 bits RAM (werkgeheugen) en enige kilobytes ROM (read only memory) en EPROM (electronically programmable read only memory) kunnen bevinden. In die laatste geheugens kunnen bij fabricage en uitgifte van de kaart programma's en geheime gegevens worden opgeslagen die daarna niet meer gewijzigd kunnen worden.

Alleen door de chip open te breken zou je de precieze inhoud van de geheugens dan nog kunnen trachten te achterhalen. Maar de chip kan zelfs zo geprogrammeerd zijn, dat hij bij zo'n aanval zichzelf vernietigt.
Zo maar kopiëren van zo'n chipkaart, zoals dat bij magneetstripkaarten kan, is dus onmogelijk, en hetzelfde geldt voor knoeien met het geheime geheugen.
Diefstal blijft natuurlijk wel een probleem, maar dat is op allerlei manieren op te lossen: een gecodeerde foto, handtekening, vingerafdruk, stemanalyse of DNA-patroon kan de koppeling tussen kaart en persoon tot stand brengen.
In de praktijk zal echter een PIN-code van vier cijfers meestal voldoende waarborgen bieden. Juist doordat de kaart een computer bevat, kan hij verkeerde PIN-code pogingen registreren, en zich na bij voorbeeld drie van die pogingen ongeldig maken.

Zero knowledge identificatie
We laten nu zien hoe zo'n *zero knowledge* identificatieprocedure in z'n werk gaat. Er is sprake van twee partijen: Anton, die z'n identiteit wil *aantonen,* en Vera, die Antons identiteit moet *verifiëren.*
Anton en Vera vertrouwen elkaar niet. Vera is bang dat Anton niet degene is voor wie hij zich uitgeeft, en Anton is bang dat Vera (of iemand die meeluistert) na de identificatie-procedure alle gegevens in handen heeft om zich op een later tijdstip als Anton voor te doen.
Dat laatste is bij voorbeeld het grote gevaar bij betaalautomaten en magneetstrippasjes. Als Anton zijn kaart in de gleuf steekt en z'n PIN-code intoetst, kunnen al zijn gegevens worden afgetapt, waarna een kwaadwillende bankbediende of een luistervink Antons pasje kan namaken en zijn rekening ongestraft kan plunderen. Bij *zero knowledge* schema's en het gebruik van chipkaarten is dat principieel onmogelijk, zoals we zullen zien.

Modulair rekenen
We nemen aan dat er een door alle partijen te vertrouwen Hoofdkwartier (HQ) is dat het systeem

beheert en de chipkaarten uitgeeft. Denk bij voorbeeld aan het hoofdkantoor van een bank of een credit-card-organisatie, of aan een ministerie.
Het HQ laat z'n computer twee priemgetallen P en Q bepalen van ongeveer honderd cijfers elk. De priemgetallen P en Q houdt HQ geheim, maar hun produkt $P \cdot Q = M$ wordt bekend gemaakt. Alle gebruikers gaan daar mee werken.

Alle berekeningen vinden plaats door *modulair rekenen* met M als *modulus.* Modulair rekenen wordt ook wel *klokrekenen* genoemd, want iedereen weet hoe je met de uren van de klok rekent. 5 uur na 9 uur is 2 uur; na het passeren van de 12 begin je weer met 1. Geleerd gezegd: $5 + 9 = 2$ *modulo* 12.
Bij klokrekenen werk je met 12 als modulus, maar op dezelfde wijze kun je elk ander getal als modulus nemen. Het komt er op neer dat je alle berekeningen 'gewoon' uitvoert, maar telkens de rest neemt na deling door M.
Modulair optellen, aftrekken, vermenigvuldigen en kwadrateren geven geen problemen. Een computer kan die bewerkingen zeer snel uitvoeren, zelfs als de modulus een getal van 200 cijfers is.

Worteltrekken
Maar *worteltrekken,* het omgekeerde van kwadrateren, brengt moeilijkheden met zich mee. Het modulaire systeem wordt dan een soort doolhof.

Ken je een getal waarvan je weet dat het *modulo M* een kwadraat is (dat is betrekkelijk eenvoudig op indirecte wijze te verifiëren), dan is het praktisch ondoenlijk om ook werkelijk zo'n wortel te vinden. Maar ken je de twee priemfactoren P en Q van M, dan kun je zo'n wortel zeer gemakkelijk berekenen! In feite kun je bewijzen dat worteltrekken *modulo M* net zo moeilijk is als het ontbinden van M in z'n priemfactoren. Kun je van willekeurige kwadraten wortels vinden, dan kun je ontbinden, en omgekeerd. Zie het artikel 'Modulair worteltrekken' op bladzijde 18.

Kaartuitgifte
Nadat HQ z'n priemgetallen P en Q gekozen heeft en de modulus $M = P \cdot Q$ bekend heeft gemaakt, kunnen de klanten komen. Stel dat Anton zich meldt met het verzoek om een chipkaart te ontvangen. Hij vult een aanvraagformulier in met daarop alle benodigde gegevens (naam, adres, geboortedatum, kredietwaardigheid, enzovoort).

Na controle worden die gegevens in een rij getallen omgezet. Om Antons privacy te beschermen, kan de rij ook nog vercijferd worden, bij voorbeeld met behulp van DES, een bekend vercijfer-algoritme dat gemakkelijk in een chip kan worden ingebouwd.
Met willekeurige getallen wordt de rij vervolgens aangevuld tot een groot getal I met net zoveel cijfers als M. Hierbij zorgt HQ ervoor dat het getal I een kwadraat *modulo M* wordt. Dat kan op betrekkelijk eenvoudige wijze gebeuren, maar het voert te ver om daarvan de details te geven.
Het getal I is Antons *openbare identificatienummer.* Hij hoeft het

niet geheim te houden, integendeel, alle I's van alle deelnemers mogen worden gepubliceerd.
Het getal I wordt ook in het geheugen van Antons chipkaart geplaatst. Maar HQ zet ook een ander getal in het geheime deel van het geheugen, namelijk een *wortel* i van I. Dat wil zeggen een getal i dat gekwadrateerd *modulo* M precies I oplevert.
HQ kan zo'n getal bepalen met behulp van P en Q. Anton krijgt die geheime priemgetallen niet te zien. Alleen het resultaat i van het worteltrekken is in zijn chip gezet. Het getal i is Antons *geheime identificatienummer*. De rol van HQ is nu uitgespeeld: Anton kan zijn kaart gaan gebruiken.

Het protocol

Het gebruik van de kaart

Hoet gaat dat in z'n werk? Als Anton zich ergens wil identificeren, presenteert hij de kaart. Vera, die de identiteit van Anton moet verifiëren, stopt de kaart in haar computer. Zij kent de modulus M, maar het is nergens voor nodig dat haar computer in verbinding staat met de centrale computer van HQ. De onafhankelijkheid van grote computernetwerken is een van de grote voordelen van dit systeem. Alle berekeningen kan Vera zelfstandig uitvoeren.
Anton heeft Vera via zijn kaart zijn openbare identificatienummer I gegeven. Vera moet verifiëren dat Antons kaart in het ontoegankelijke geheugendeel een getal i bevat waarvoor geldt dat $i^2 = I$ *modulo* M. Maar als i bekend wordt, kan Vera de kaart van Anton vervalsen. Daarom doen ze het anders.

Een groot aantal malen (bij voorbeeld honderd keer) herhalen ze het volgende vraag-en-antwoordspel:

1. Anton kiest een willekeurig getal x en bepaalt het kwadraat $X = x^2$ *modulo* M. Hij deelt dat kwadraat X aan Vera mede.
2. Vera mag één van de volgende vragen stellen (maar niet beide!):
   a. Wat is x?
   b. Wat is $x \cdot i$?
   Anton beantwoordt die vraag.
3. Vera verifieert Antons antwoord door in geval (a) te controleren dat $x^2 = X$, en in geval (b) dat $(x \cdot i)^2 = X \cdot I$.

In werkelijkheid wordt het hele spel natuurlijk zelfstandig door de chip van Anton en de computer van Vera uitgevoerd. Het geheel duurt slechts een paar seconden.

Bedrieger

Stel dat Anton een bedrieger is die i niet kent. Hoe groot is dan de kans dat hij zo'n test doorstaat? Hij kan gokken welke keuze Vera gaat doen.
Gokt hij op (a), dan kan hij in stap 1 de normale procedure kiezen. Als Vera inderdaad (a) kiest, zit hij goed.
Verwacht hij dat Vera (b) kiest, dan kan hij bij stap 1 een getal y kiezen, het kwadraat $Y = y^2$ *mo-*

dulo M berekenen, en dan aan Vera het quotiënt $X = Y/I$ mededelen. Kiest Vera inderdaad vraag (b),dan zit hij goed als hij het antwoord *y* geeft, want Vera verifieert dan dat $y^2 = Y = X \cdot I$.
Maar in beide gevallen is hij de klos als Vera de andere vraag stelt. Zijn overlevingskans bij één ronde is dus 1 op 2. De overlevingskans bij *honderd* rondes is echter slechts 1 op twee-tot-de-honderdste!
Vera hoeft dus niet bang te zijn dat Anton een bedrieger is als hij alle tests doorstaat. Zij verklaart Antons identiteitskaart dan geldig.

Weet Vera iets?
Weet Vera na afloop iets over Antons geheime nummer *i*? De keren dat ze vraag (a) koos, speelde *i* helemaal geen rol, en de keren dat ze vraag (b) koos, was *i* veilig verpakt in het produkt $x \cdot i$; omdat ze *x* niet kende, kon ze *i* ook niet achterhalen.

Voor Anton is het van groot belang de keuzen van *x* op een onvoorspelbare manier uit te voeren. Alleen in dat geval kan Vera niets over *i* te weten komen.
In het extreme geval dat hij zo stom is om Vera twee maal dezelfde *X* te presenteren, kan Vera door beide vragen te stellen zowel *x* als $x \cdot i$ te weten komen, en dan kent ze na deling ook *i*.

Het bovenstaande geeft in grote lijnen het protocol weer van een 'zero knowledge proof of identity'. Door kleine modificaties kan men de snelheid van de procedure nog aanzienlijk verhogen.

Bruikbaarheid

Hoe bruikbaar is zo'n systeem in de praktijk? Chipkaarten zijn duurder dan magneetstrippasjes, maar de kosten vormen geen onoverkomelijk probleem. Bij massaal gebruik zullen die kosten ook sterk dalen.
Wel is het nodig dat overal waar met deze systemen gewerkt wordt verificatie-computertjes aanwezig zijn. Maar die hoeven slechts een simpele rekenchip te bevatten; verbindingen met een centrale computer en grote geheugencapaciteiten zijn niet vereist. Grote kosten zijn daar dus niet aan verbonden.

Gevaar
Het enige grote gevaar dat de methode bedreigt komt van de wiskunde zelf. Misschien lukt het slimme wiskundigen om snelle ontbindingsalgoritmen te ontwerpen. Dan stort de veiligheid van het systeem in elkaar, want dan kun je *M* in z'n priemfactoren *P* en *Q* ontbinden, en daarmee wordt worteltrekken modulo *M* een fluitje van een cent.
Als dat gebeurt, zijn er echter nog allerlei andere wiskundige problemen voorhanden die voor deze zelfde cryptografische doeleinden gebruikt kunnen worden. Er zal waarschijnlijk steeds een rivaliteit blijven tussen de wiskundigen die nieuwe systemen ontwerpen, en de wiskundigen die ze zullen trachten te kraken. □

Overbodige nullen op postzegels

Als je er op gaat letten, blijkt het symbool ' 0 ' in de notatie van getallen niet altijd op een consequente manier voor te komen. En soms wordt die 0 ook anders gebruikt dan wat je daarover op school (misschien) geleerd hebt. De voorbeelden halen we van postzegels en poststempels.

Nul helen en een breukdeel
Bij het opschrijven van de breuk 'een half' kiezen we meestal tussen de *breukstreep*-notatie

$\frac{1}{2}$ (of $^1/_2$ of 1/2)

en de *komma*-notatie

0,5 (of 0.5).

Omdat iedereen dit haast altijd zo noteert, zul je je nooit afgevraagd hebben waarom het ontbreken van gehelen in de kommanotatie *wél*, maar in de breukstreepnotatie *niét* door het symbool 0 wordt aangegeven.

Logischer lijkt het om ofwel te kiezen voor

$\frac{1}{2}$ en ,5

ofwel voor

$0\ \frac{1}{2}$ en 0,5 .

Waarom gebeurt dat niet?
Ik weet het niet. Misschien is het min of meer toevallig historisch zo gegroeid. Misschien ook dat gedacht wordt dat de komma (en de punt net zo) zonder nul ervóór, in een lopende tekst verwarrend kan zijn. Omdat diezelfde komma ook als gewoon leesteken voor kan komen.

Afwijkingen van het gangbare gebruik zijn te vinden op twee zegels van Australië uit 1950 en 1955, beide met de waarde

1 shilling $0\ \frac{1}{2}$ pence.

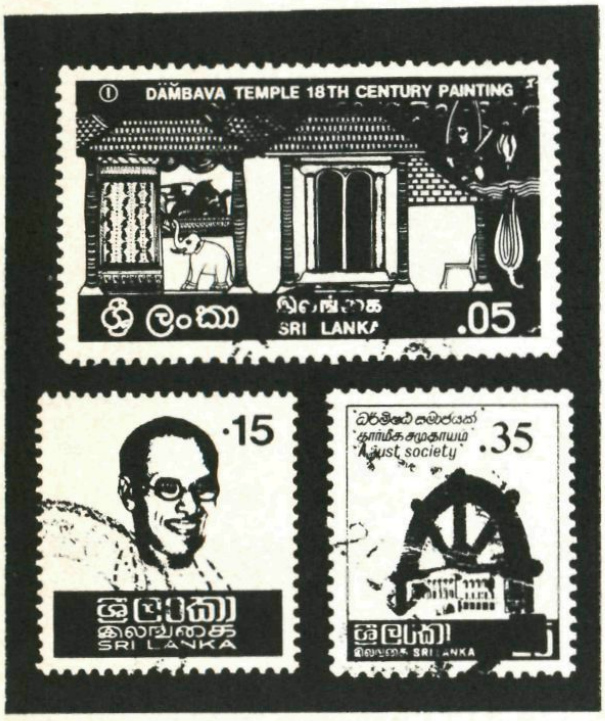
(Het woord shilling werd vroeger met een zogenaamde 'lange s' geschreven, die in de afkorting vervormde tot een schuine streep of tot een hoog geplaatst accent.)

Merkwaardige manieren om een 'halve cent' aan te duiden vinden we verder in Panama (1921) en in een omwaarderings-opdruk op zegels van Angola (1919). In plaats van
0,005 balboa en 0,005 escudo staat er
B/0.00$\frac{1}{2}$ en $ 00,5 !

Is 0.00$\frac{1}{2}$ wat anders als 0.0$\frac{1}{2}$?

$00,5 =

Afwijkingen in een andere richting (géén nul voor de komma of de punt) komen consequent voor op de zegels van Sri Lanka van na 1972. De decimale punt staat daar soms op halve hoogte in plaats van gewoon op de regel.



Nog iets dergelijks komt voor op zegels van Portugal. In plaats van de decimale komma of punt staat op die positie vaak het teken $ voor de munteenheid *escudo*. Bij waarden onder één volle escudo wordt nooit een 0 genoteerd ter aanduiding van het ontbreken van gehelen.

Nullen links van de helen
Op school leer je om niet 03 te schrijven, maar 3. En niet 0025 maar 25. De regel is dat zulke 'linkernullen' worden weggelaten. Een aantal uitzonderingen volgen hieronder.

— Er bestaat een zegel van Ceylon/Sri Lanka uit 1972 met als waardeaanduiding:

CENTS 05

Dit lijkt een overgangsvorm te zijn tussen het eerder gebruikelijke 'CENTS 5' en het latere ' .05 '

— Het zelfde zien we in een opdruk op zegels van Spaans Guinee

(1908) ter waarde van *5 centesimos*.

— Op de (rode) afdrukken van frankeermachines zijn regelmatig linkernullen te zien.

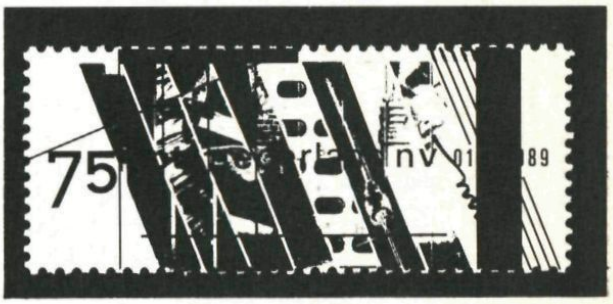
— Linkernullen komen soms ook voor in tijdsaanduidingen (uren-, minuten- en secondenaantallen) en in datumaanduidingen (dag- en maandnummers).
Een Hongaarse zegel uit 1959 geeft het landingstijdstip van een Russische sonde op de maan aan als:

$22^h\,02'\,34''$

(= 22 uur 2 minuut 34 seconde).

— Op de Nederlandse PTT-zegel van 1989 staat (bijna onleesbaar klein) als datum van verzelfstandiging:

01 01 1989



— In sommige landen kunnen in de poststempels linkernullen voorkomen vóór het dag- of maandnummer. Bijvoorbeeld België (03.07.89-17), de DDR (06.04.82) en ook Noorwegen.

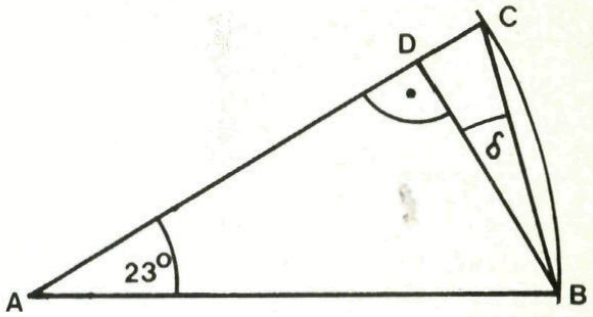
— In Nederland komen zulke linkernullen voorzover bekend (nog) niet voor in de gewone (zwarte) stempels. Echter wél in de rode datum-stempeling van sommige frankeermachines:

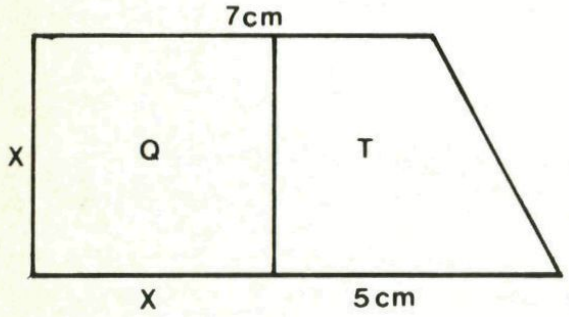
Oproep
Het toevoegen van (min of meer overbodige) linkernullen lijkt me een nog niet zo erg oud gebruik. Ik ben benieuwd of er lezers zijn die mij kunnen wijzen op wat oudere (zo oud mogelijke) voorkomens ervan. Op postzegels, poststempels, of ook op andere plaatsen.

In een vervolg-stukje zullen we de overbodige nullen ná de komma nader onder de loep nemen. □

Bekijk het even

A is middelpunt van de cirkelboog. *BD* staat loodrecht op *AC*.
Bereken δ. □



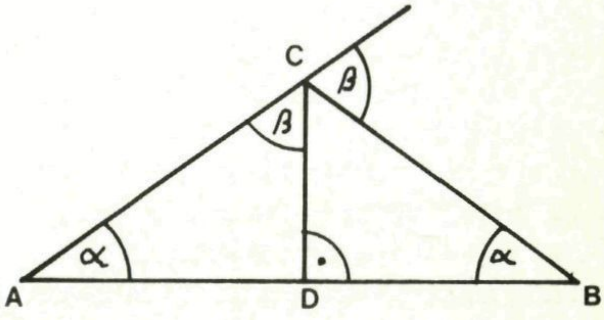


Bekijk het even

De oppervlakte van het vierkant *Q* is gelijk aan de oppervlakte van het trapezium *T*.
Bereken *x*. □

Bekijk het even

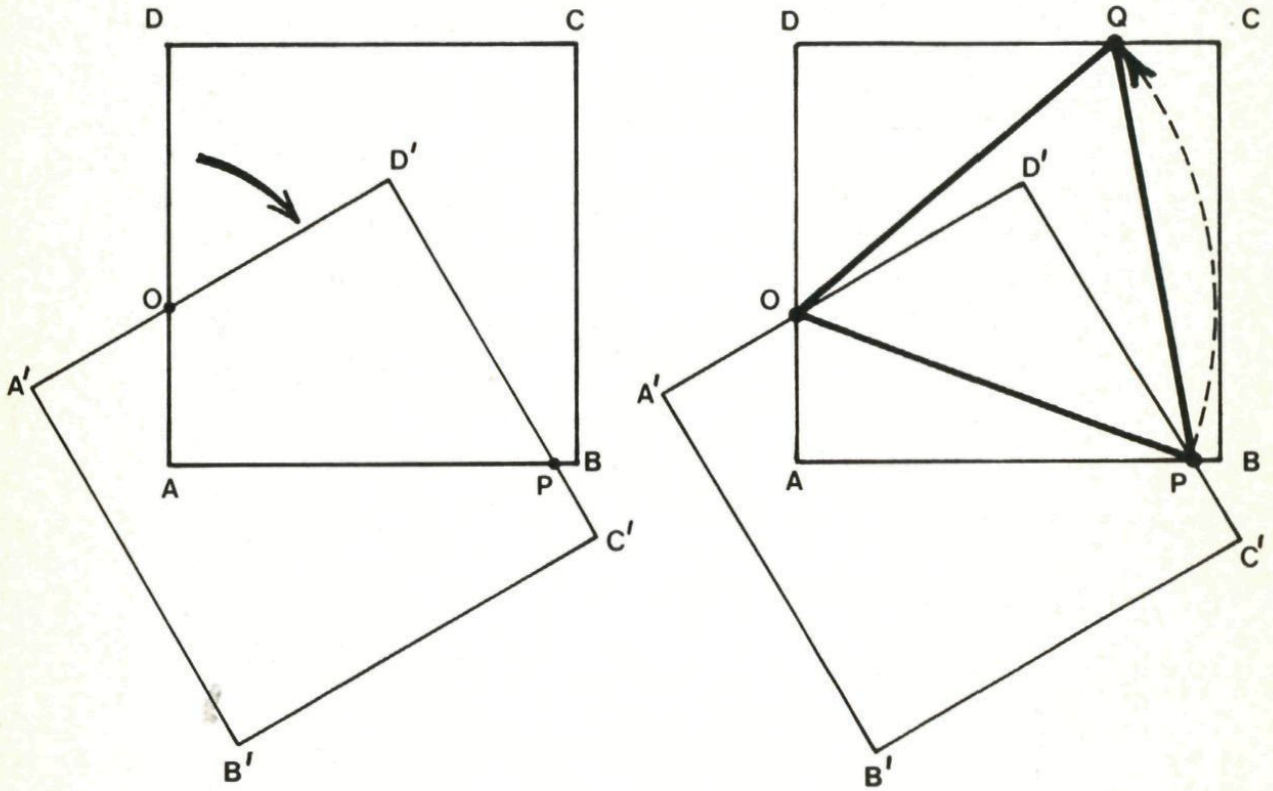
CD staat loodrecht op *AB*.
Bereken α en β. □



Driehoek in vierkant

Construeer een gelijkzijdige driehoek waarvan de hoekpunten op drie verschillende zijden van een gegeven vierkant *ABCD* liggen.

Probeer maar eens. Het zal echt niet meevallen om zo'n driehoek in een vierkant te construeren. Maar als je de hieronder beschreven methode hebt gezien, zul je toe moeten geven dat het toch eigenlijk heel eenvoudig is. Bovendien is het bewijs dat de met die methode verkregen driehoek ook werkelijk gelijkzijdig is, zo mogelijk nog eenvoudiger!



Figuur 1. Na keuze van O *volgt een rotatie van vierkant* ABCD *over 60° (links). Dit levert een punt* P *dat kan worden gezien als het beeldpunt van* Q *(rechts).*

Methode

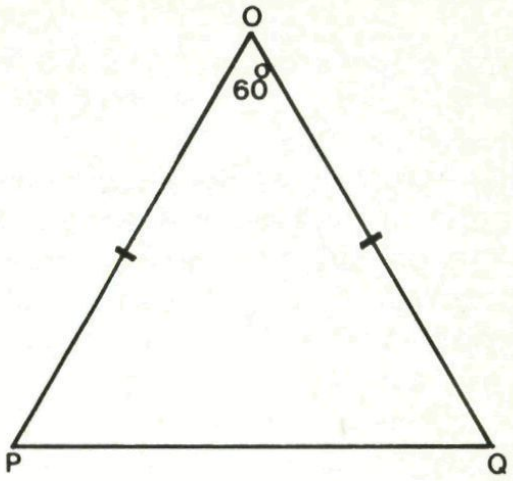
Kies op een van de zijden van het gegeven vierkant, zeg *AD*, een willekeurig punt *O* (figuur 1). Neem dit punt *O* als centrum van rotatie en roteer *ABCD* over een hoek van 60° om *O*. De beeldfiguur wordt dan een vierkant *A'B'C'D'*. Met geodriehoek en passer of zelfs alleen met een passer is dit eenvoudig uit te voeren. Noem het snijpunt van *C'D'* met een van de zijden van het oorspronkelijke vierkant (hier de zijde *AB*) *P*.

Het punt *P* ligt op *C'D'* dus is *P* het beeldpunt van een punt *Q* op *DC*. Dit punt *Q* kan worden verkregen door de passerpunt in *O* te zetten

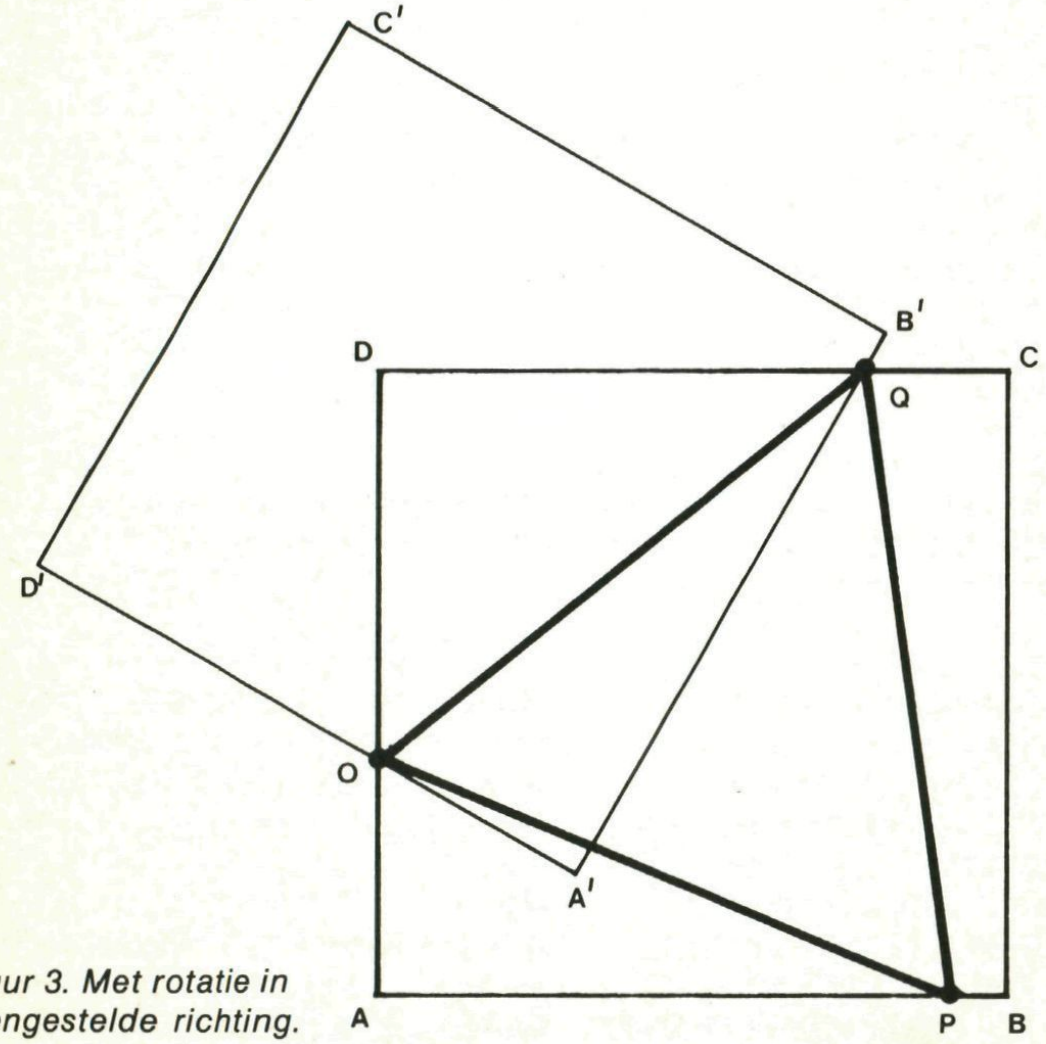
en *OP* om te cirkelen. Driehoek *OPQ* is dan de gevraagde gelijkzijdige driehoek.

Bewijs
P is het beeldpunt van Q bij rotatie van 60° om *O*. Dus hoek *POQ* is 60° en *OP* is gelijk aan *OQ*. Nu is driehoek *OPQ* gelijkbenig met een tophoek van 60° (figuur 2). Maar dan zijn ook de twee basishoeken van die driehoek 60°, en zijn de drie zijden gelijk.

Figuur 2



In tegengestelde richting
Na keuze van *O* kan de rotatie over 60° ook in tegengestelde richting worden uitgevoerd (figuur 3). In dat geval wordt *Q* op *A'B'* gevonden. Dat punt *Q* is nu omgekeerd te beschouwen als het beeldpunt van een punt *P* op *AB*. Enzovoort.
Uitgaande van eenzelfde punt *O* wordt precies dezelfde driehoek *OPQ* verkregen. □



Figuur 3. Met rotatie in tegengestelde richting.

Modulair worteltrekken

In het artikel 'Zero knowledge proofs' hebben we gezien dat 'veilige' wachtwoord procedures voor een deel berusten op rekenen modulo een groot getal M dat het product is van twee grote priemgetallen P en Q. Met name de moeilijkheid van *modulair worteltrekken* is de basis van de veiligheid van het systeem. In dit artikel geven we wat achtergrondinformatie over modulair rekenen.

Kilometerteller

Denk om te beginnen eens aan de kilometerteller van een auto. Meestal laat die zes cijfers zien; de standen lopen van 000 000 tot 999 999. Er zijn dan 1 miljoen getallen op die teller mogelijk. Je kunt er mee rekenen: optellen, aftrekken (terugdraaien), vermenigvuldigen (herhaald optellen), en zelfs machtsverheffen (herhaald vermenigvuldigen). In het bijzonder kun je ook kwadrateren.
Kom je over de 999 999 heen, dan springt de teller weer op 000 000 en telt dan verder. De gewone regels blijven geldig mits je, in geleerde termen gezegd, 'modulo 1 miljoen' rekent. Nu is 1 miljoen wel erg groot; je kunt ook een kleiner getal als *modulus* nemen. Een teller met slechts twee cijferposities rekent 'modulo 100', en kijken we op de klok, dan rekenen we 'modulo 12'.

Rekenen

Elke modulus m levert zo dus een getallensysteem op dat bestaat uit de getallen 0, 1, 2, ..., m-1 (het is gebruikelijk om met 0 te beginnen, net als bij de kilometerteller). We noemen dat systeem Z_m.
Je kunt in Z_m optellen, aftrekken, vermenigvuldigen en machtsverheffen, net als bij het gewone systeem van de gehele getallen. Het komt er op neer dat je gewoon rekent, en dan telkens de rest bepaalt na deling door m.

Priemgetal als modulus

De aard van de modulus bepaalt voor een groot deel de aard van het getallensysteem Z_m. Het maakt met name nogal wat uit of m een *priemgetal* is of niet. We illustreren dat aan de hand van de vermenigvuldigingstabellen van Z_7 en Z_{12}.
In figuur 1 staat de tabel van Z_7. De derde rij bevat bij voorbeeld in telegramstijl de 'tafel van 3' modulo 7: 3, 6, 2, 5, 1, 4, 0. Alle getallen uit het systeem komen in die rij voor.
Dat geldt ook voor alle andere tafels, behalve natuurlijk voor de tafel van 0. Die hebben we weggelaten, want die bestaat alleen maar uit nullen.
Dat alle getallen in alle tafels voorkomen, heeft de merkwaardige consequentie dat je in dit getallensysteem *altijd zonder rest kunt delen!* Zo is bij voorbeeld $5/4 = 3$ want $5 = 4 \cdot 3$, en $2/5 = 6$ want $2 = 5 \cdot 6$. Delen door nul is natuurlijk ook in dit systeem onmogelijk, maar voor de rest gaat elke deling op.
Je kunt bewijzen dat deze verschijnselen optreden in alle getalsystemen Z_p waarvoor p een

priemgetal is. In elke rij van de vermenigvuldigingstabel komen dan alle getallen uit het systeem voor, en je kunt dus ook altijd zonder rest delen.

Modulus geen priemgetal

Heel anders is de situatie in Z_{12}. In figuur 2 zie je dat daar alleen in de tafels van 1, 5, 7 en 11 alle getallen voorkomen, de andere tafels bevatten slechts een beperkte selectie. In dit getallensysteem gaan delingen dus niet altijd op.

Kwadrateren en worteltrekken

Hoe zit het met kwadrateren? In figuur 1 staan de kwadraten op de hoofddiagonaal: $1 \cdot 1 = 1$, $2 \cdot 2 = 4$, $3 \cdot 3 = 2$, $4 \cdot 4 = 2$, $5 \cdot 5 = 4$ en $6 \cdot 6 = 1$. Niet alle getallen komen voor als kwadraat; de kwadraten zijn 1, 4 en 2. En elk kwadraat heeft *twee* wortels: 4 heeft bij voorbeeld de wortels 2 en 5.
Ook dat is weer karakteristiek voor alle getallensystemen Z_p waarvoor p een priemgetal groter dan 2 is. Elk kwadraat (ongelijk 0) heeft altijd *twee* wortels.

Bewijs Een bewijs hiervan is heel gemakkelijk. Laat een kwadraat a^2 van een getal a uit het systeem gegeven zijn. Stel dat een getal b uit het systeem hetzelfde kwadraat heeft, dus $b^2 = a^2$ modulo p. Dan is $b^2 - a^2 = (b-a)(b+a)$ een geheel veelvoud van p.

Maar omdat p een priemgetal is, moet p dan een deler zijn van $b-a$ of van $b+a$. Als a en b beide kleiner dan p zijn, moet dus gelden: $b = a$ óf $b = p-a$.
In het laatste geval zijn a en b verschillend, want p is oneven (elk priemgetal groter dan 2 is oneven).

Hoe zit het als de modulus geen priemgetal is? Kijk weer naar figuur 2. Daar staan de kwadraten modulo 12 op de hoofddiagonaal. Het zijn er vier: 0, 1, 4 en 9. De kwadraten 1 en 4 komen *vier* keer voor, 9 komt twee keer voor en 0 ook: $0 = 6^2 = 0^2$.

Beperking

In het algemeen is de situatie als de modulus geen priemgetal is nogal gecompliceerd. We beperken ons tot het geval waar we mee begonnen zijn:

x	2x	3x	4x	5x	6x	7x	(= 0x)
1	2	3	4	5	6	0	
2	4	6	1	3	5	0	
3	6	2	5	1	4	0	
4	1	5	2	6	3	0	
5	3	1	6	4	2	0	
6	5	4	3	2	1	0	

Figuur 1. Vermenigvuldigingstabel van Z_7.

x	2x	3x	4x	5x	6x	7x	8x	9x	10x	11x	12x	(= 0x)
1	2	3	4	5	6	7	8	9	10	11	0	
2	4	6	8	10	0	2	4	6	8	10	0	
3	6	9	0	3	6	9	0	3	6	9	0	
4	8	0	4	8	0	4	8	0	4	8	0	
5	10	3	8	1	6	11	4	9	2	7	0	
6	0	6	0	6	0	6	0	6	0	6	0	
7	2	9	4	11	6	1	8	3	10	5	0	
8	4	0	8	4	0	8	4	0	8	4	0	
9	6	3	0	9	6	3	0	9	6	3	0	
10	8	6	4	2	0	10	8	6	4	2	0	
11	10	9	8	7	6	5	4	3	2	1	0	

Figuur 2. Vermenigvuldigingstabel van Z_{12}.

Een modulus M die het product is van *twee* grote priemgetallen P en Q.

Je kunt bewijzen dat dan iets meer dan *een kwart* van de getallen uit het systeem Z_M een kwadraat is, en dat elk kwadraat (ongelijk aan 0 modulo M)dan hoogstens vier wortels heeft. Ken je de priemfactoren P en Q, dan kun je die wortels betrekkelijk snel bepalen, maar de methode waarmee dat gedaan wordt, is te ingewikkeld om hier uit te leggen.

De kunst

Dat een kwadraat hoogstens vier wortels heeft, is echter niet zo moeilijk in te zien. Stel maar weer dat $b^2 = a^2$ modulo M. Dan is $(b-a)\ (b+a)$ een geheel veelvoud van M. Er zijn nu vier mogelijkheden:

1. $b-a$ is een veelvoud van M. Dan zijn b en a modulo M gelijk.
2. $b+a$ is een veelvoud van M. Dan is $b = M - a$ modulo M.
3. $b-a$ is een veelvoud van P, en $b+a$ is een veelvoud van Q.
4. $b-a$ is een veelvoud van Q, en $b+a$ is een veelvoud van P.

Je kunt bewijzen dat de mogelijkheden 3 en 4 bij gegeven a elk precies één getal b modulo M opleveren. In veel gevallen zijn die uitkomsten anders dan de uitkomsten die je bij 1 en 2 hebt gekregen, dus dan vind je bij gegeven a^2 *vier* verschillende wortels. Of liever gezegd, die wortels zijn er, maar het *vinden* ervan is de grote kunst!

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

Figuur 3. Kwadraten en wortels modulo 35.

De praktijk

Als M betrekkelijk klein is, zijn er geen problemen. Je maakt dan gewoon een tabel. In figuur 3 staan bij voorbeeld de kwadraten modulo 35 met daarbij de wortels. De modulus is hier het produkt van de kleine priemfactoren 5 en 7.

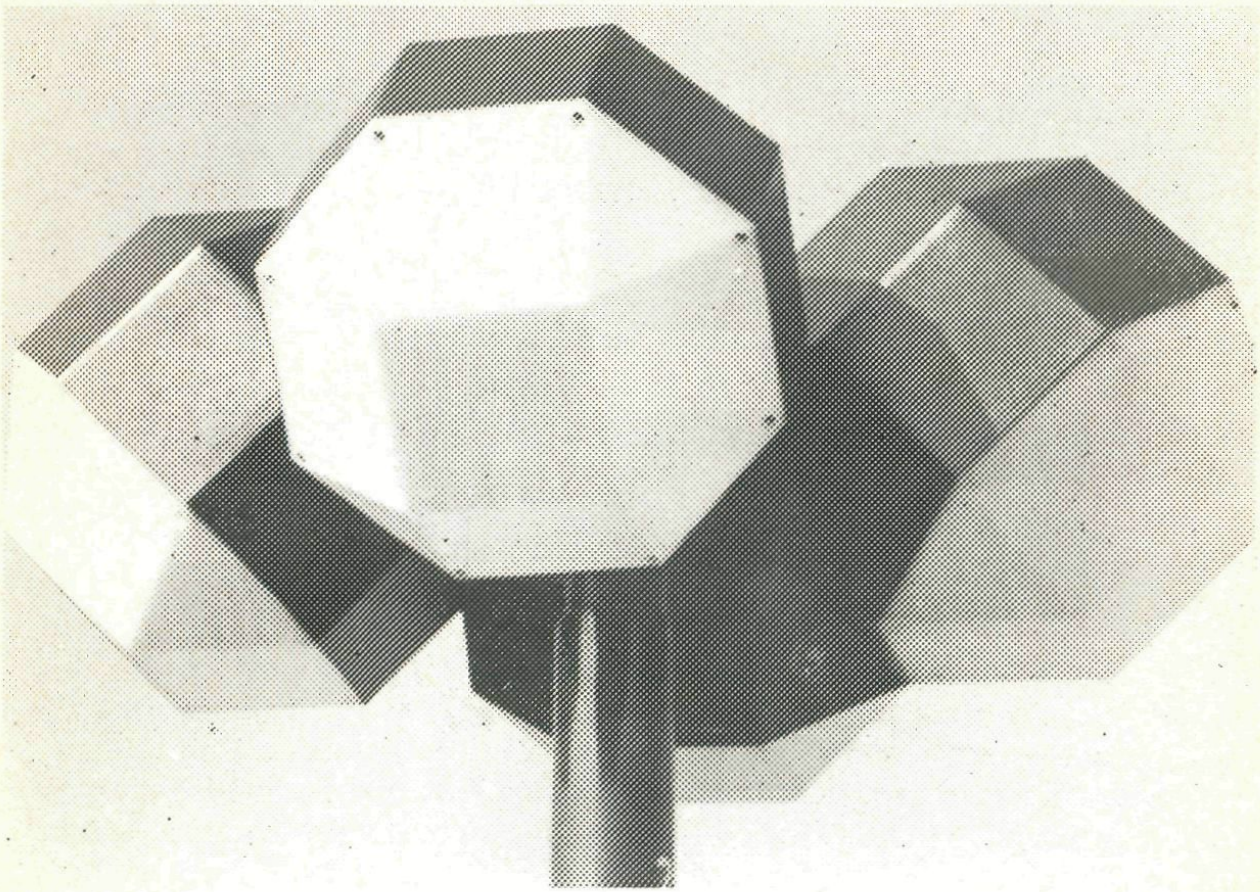
Maar als M een getal van 200 cijfers is en de grote priemgetallen P en Q worden geheim gehouden, dan blijken zulke wortels *in de praktijk onvindbaar te zijn*, zelfs met de krachtigste computers. Iemand die zo'n wortel kent, heeft dus een geheim dat niemand hem op slinkse wijze kan ontfutselen. Dat is de basis van de veilige wachtwoordprocedures.

Denkertjes

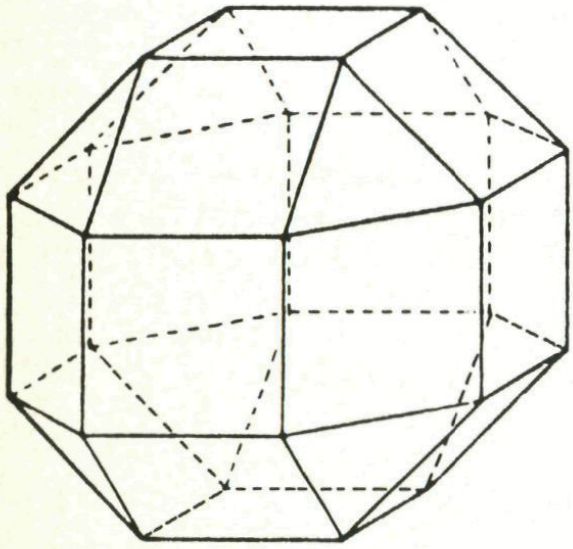
Nog een paar denkertjes: In figuur 3 zie je dat de kwadraten die slechts *twee* wortels hebben, precies de kwadraten zijn die deelbaar zijn door 5 of 7. Kun je dat verklaren?

En snap je ook waarom bij *zeer grote* priemfactoren P en Q het overgrote deel van de kwadraten *vier* wortels moet hebben? □

Lantaarns met opvallende kappen



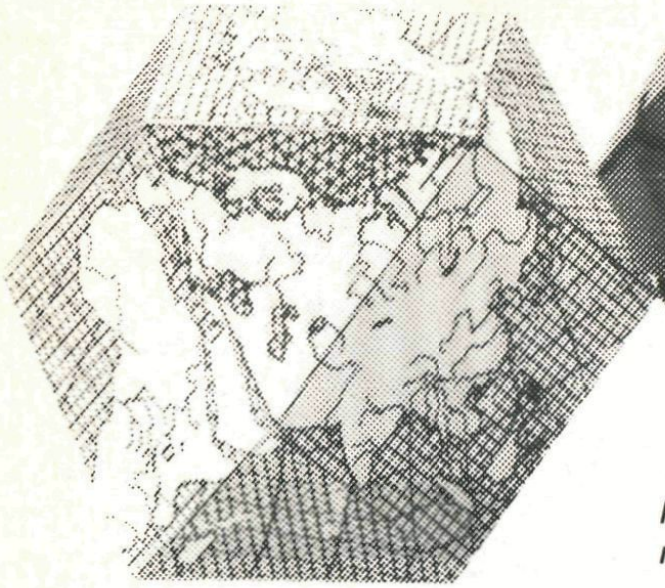
Figuur 1. Lantaarn ontworpen door Ninaber-Peters-Krouwel, Industrial Design, Delft. In de handel gebracht door de firma Raak te Aalsmeer.

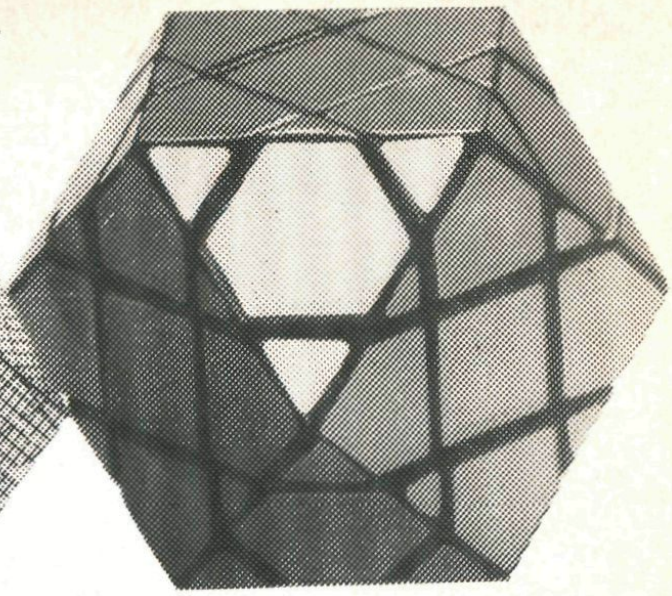


Figuur 2. Rhombikuboctaëder met 26 zijvlakken, 48 ribben en 24 hoekpunten.

Figuur 3. Voetbal. Afgeleid van een halfregelmatig veelvlak met 32 zijvlakken, 90 ribben en 60 hoekpunten.

Figuur 4. De 'dymaxion' globe (halfregelmatig veertienvlak).





Figuur 5. Een puzzel van Rubik (halfregelmatig veertienvlak).

In een plaatselijk winkelcentrum ontdekte *B.J.M. Roovers* uit Eindhoven lantaarns met een opvallend uiterlijk (figuur 1). De vier kappen van zo'n lantaarn hebben de vorm van een veelvlak dat je niet dikwijls in kunst en kunstnijverheid tegenkomt. Het is een zogenaamd halfregelmatig of archimedisch veelvlak. Officieel wordt dit veelvlak *rhombikuboctaëder* genoemd. Het wordt begrensd door 26 zijvlakken: 8 regelmatige driehoeken en 18 vierkanten (figuur 2). Verder heeft het 48 even lange ribben en 24 hoekpunten.
Naast de rhombikuboctaëder zijn er nog twaalf andere halfregelmatige veelvlakken. Die komen eveneens zelden voor in kunst of kunstnijverheid. Wie kent naast deze lantaarns, een voetbal (figuur 3), de 'dymaxion'-globe van Buckminster Fuller (figuur 4 en Pythagoras 25-5), een puzzel van Rubik (figuur 5) en een koekblik (zie een van de kaderstukjes) andere voorbeelden?
Laat het ons eens weten.
De vijf regelmatige veelvlakken zul je waarschijnlijk wel kennen. De dertien halfregelmatige veelvlakken misschien niet (allemaal). Via de kaderstukjes kun je er daarom (opnieuw) kennis mee maken. Eerst worden de eigenschappen van de regelmatige of platonische veelvlakken op een rijtje gezet. Door die wat nader onder de loep te nemen, komen we vanzelf bij de halfregelmatige veelvlakken terecht. □

De platonische veelvlakken

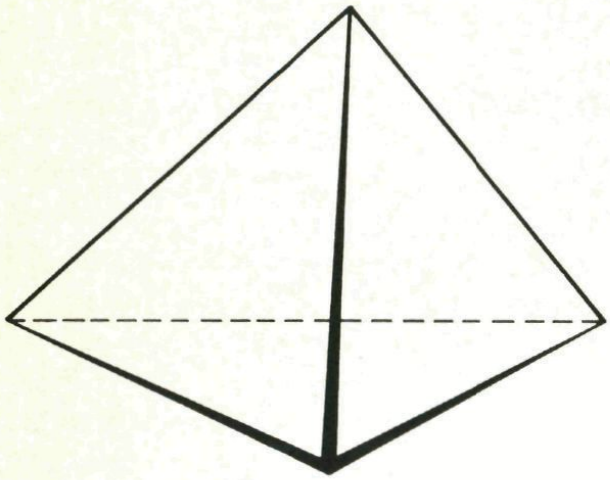
Dit zijn de bekende vijf regelmatige veelvlakken. De Griekse filosoof Plato (427-347 v.C.) maakte er melding van. Daarom worden ze ook wel naar hem platonische veelvlakken genoemd. Drie er van (de kubus, het regelmatig vier- en twaalfvlak) waren echter al rond 500 v.C. bij leerlingen van Pythagoras bekend.

Eigenschappen

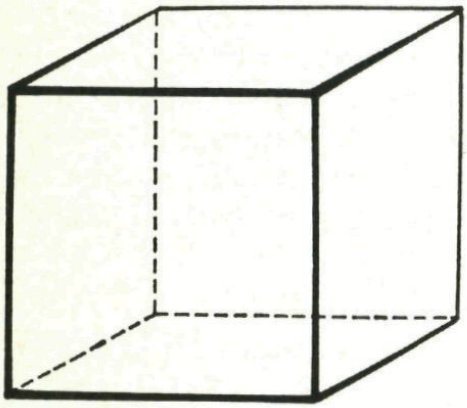
De vijf regelmatige veelvlakken zijn de enige veelvlakken die aan de volgende eigenschappen voldoen:

1 Alle zijvlakken zijn congruent;
2 Alle zijvlakken zijn regelmatige veelhoeken;
3 In *elk* hoekpunt komt *dezelfde* schikking van vlakke hoeken voor;
4 Er gaat een bol door *alle* hoekpunten.

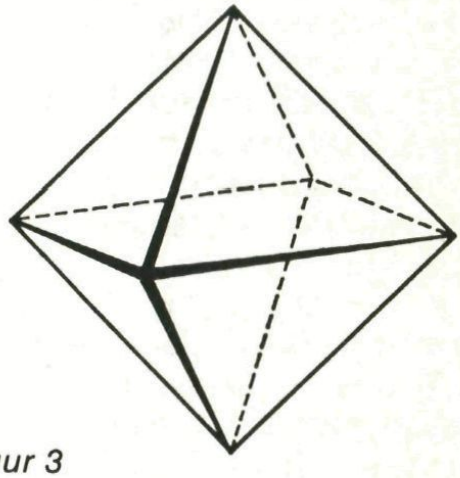
Om deze eigenschappen te kunnen controleren zijn de platonische veelvlakken alle vijf nog eens afgebeeld. Het regelmatig viervlak (tetraëder) in figuur 1, de kubus in figuur 2, het regelmatig achtvlak (octaëder) in figuur 3, het regelmatig twaalfvlak (dodecaëder) in figuur 4 en ten slotte het regelmatig twintigvlak (icosaëder) in figuur 5. □



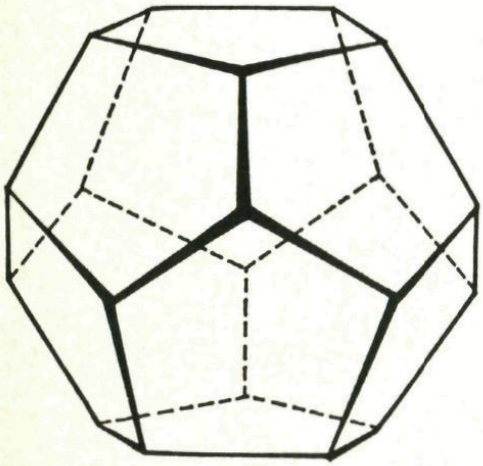
Figuur 1



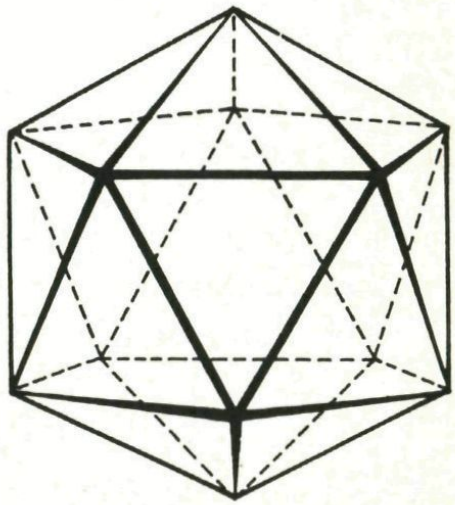
Figuur 2



Figuur 3



Figuur 4



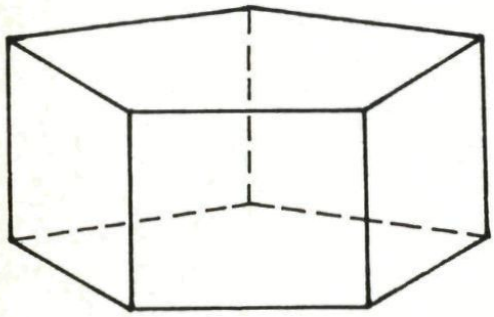
Figuur 5

De archimedische veelvlakken

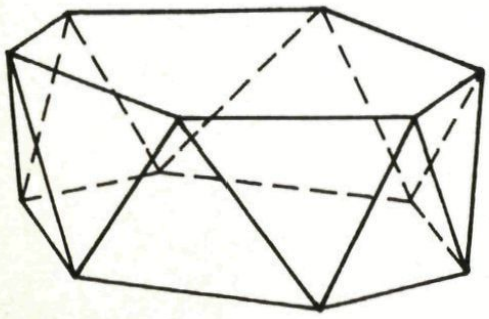
Alle dertien halfregelmatige veelvlakken zijn al van oudsher bekend. De Griek Archimedes (287-212 v.C.) kende ze reeds. Daarom worden ze ook we archimedische veelvlakken genoemd.

Een minder

Zoals de naam al aangeeft, hebben halfregelmatige veelvlakken bijna dezelfde eigenschappen als de regelmatige. Bij de halfregelmatige veelvlakken komt alleen de eerste eigenschap te vervallen.
De zijvlakken zijn nu dus verschillende, maar nog wel regelmatige veelhoeken. In de hoekpunten komen dan ook verschillende regelmatige veelhoeken samen. Maar wel zodanig dat de hoekpunten congruent zijn (eigenschap 3). Rond elk hoekpunt gaande kom je die verschillende regelmatige veelhoeken steeds in dezelfde aantallen en in dezelfde volgorde tegen. Controleer dat maar eens bij de rhombikuboctaëder.



Figuur 1. Een regelmatig prisma.



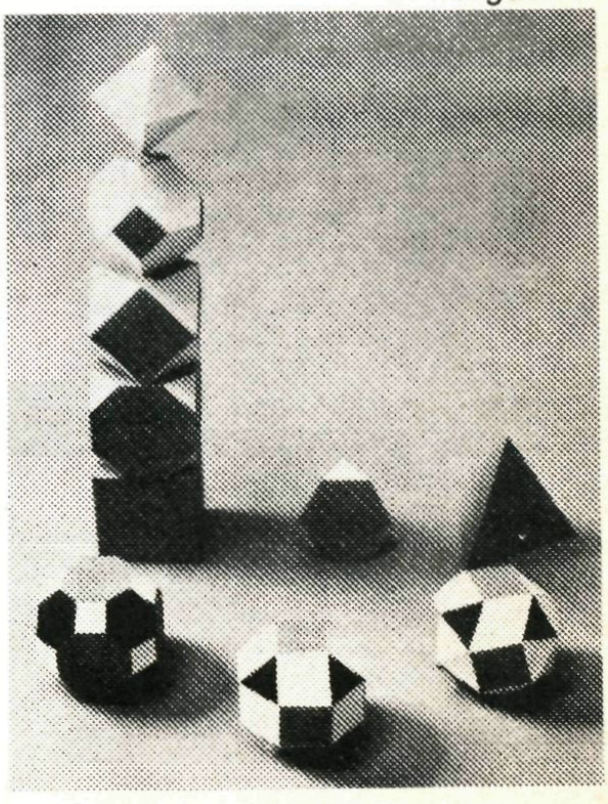
Figuur 2. Een regelmatig antiprisma.

Oneindig veel

Er zijn oneindig veel veelvlakken die aan deze eigenschappen voldoen. Om te beginnen alle *regelmatige prisma's* (figuur 1). Daarbij zijn grond- en bovenvlak regelmatige *n*-hoeken, die in evenwijdige vlakken liggen met de hoekpunten precies boven elkaar. De afstand tussen grond- en bovenvlak is gelijk aan de zijden van de *n*-hoeken. De opstaande zijvlakken zijn dus steeds congruente vierkanten.

De regelmatige *n*-hoeken die het grond- en het bovenvlak vormen, kunnen ook een tikkeltje gedraaid zijn ten opzichte van elkaar (figuur 2). Zo ontstaat een *regelmatig antiprisma,* ook wel *regelmatig prismoïde* genoemd.

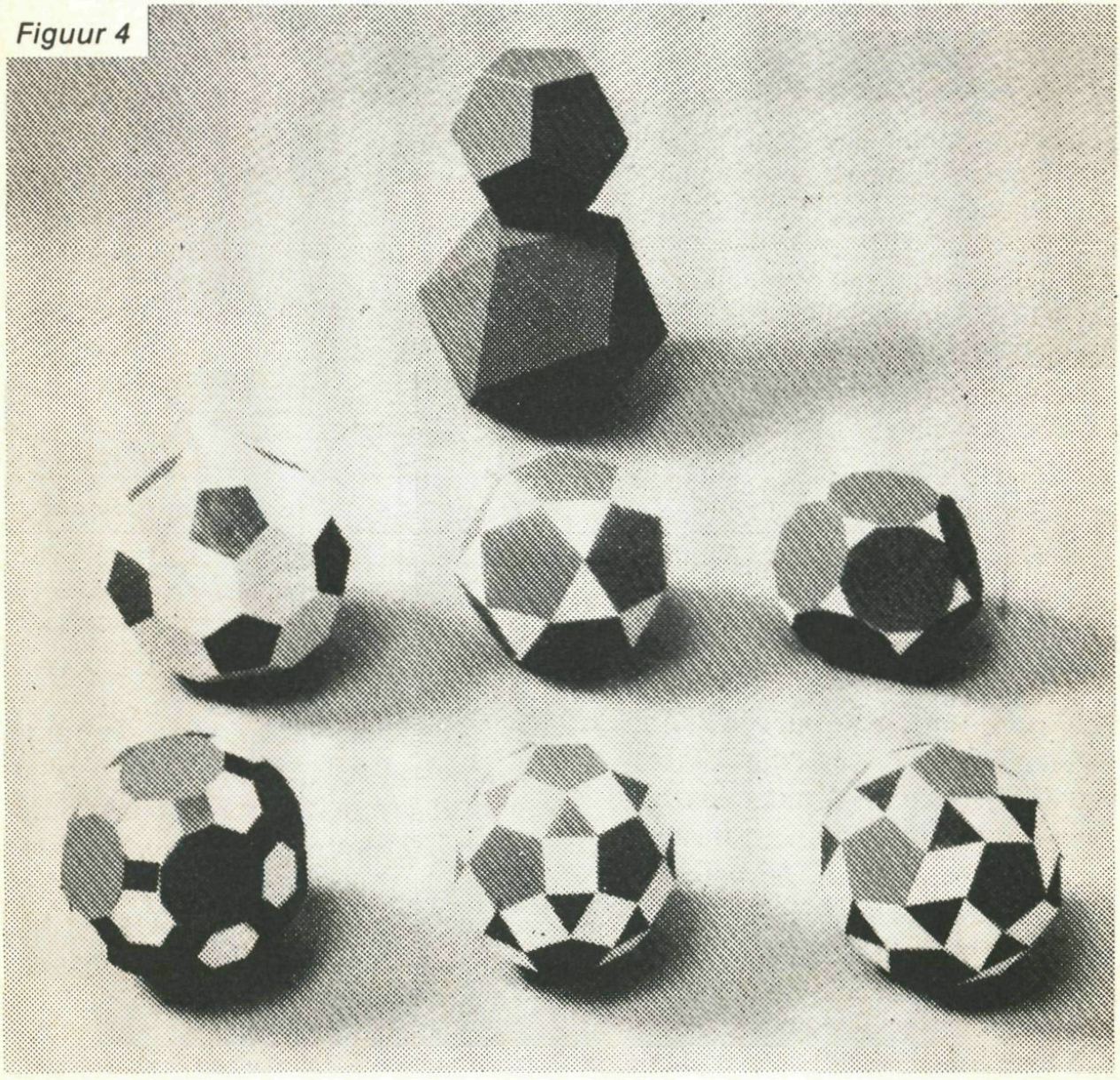
Figuur 3

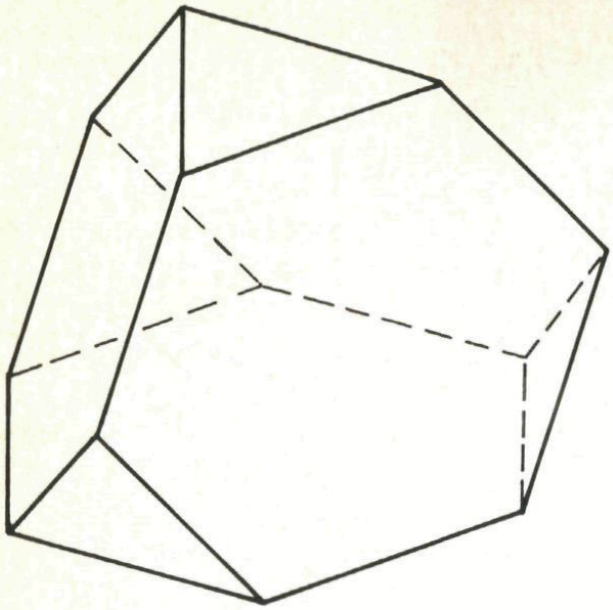


Elk hoekpunt van het bovenvlak ligt dan precies midden tussen de twee hoekpunten van het grondvlak waarmee het wordt verbonden. De opstaande zijvlakken zijn nu dus regelmatige driekhoeken.
Regelmatige prisma's en regelmatige antiprisma's zijn wel te vinden in de vorm van koekblikken.

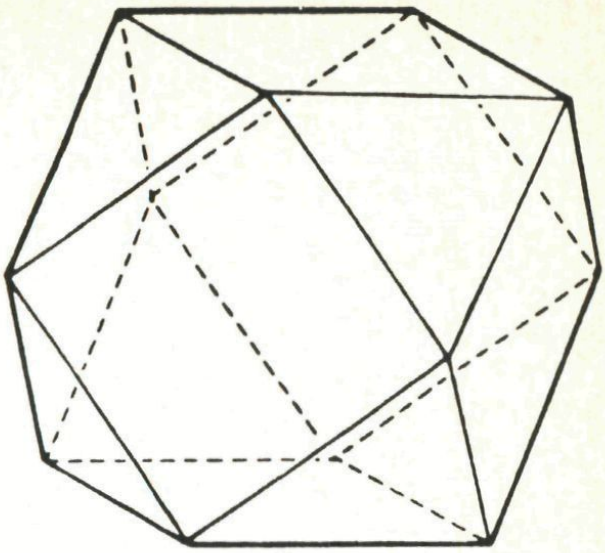
Beperking
De regelmatige prisma's en de regelmatige antiprisma's hebben meer een 'schijf-' dan een 'bol-'karakter. Daarom telde Archimedes ze liever niet mee. Afgezien van die prisma's en antiprisma's zijn er nog slechts dertien andere halfregelmatige veelvlakken. Dat het er precies dertien kunnen zijn, is te bewijzen. Het bewijs wordt hier echter achterwege gelaten.
In de figuren 3 en 4 zijn de dertien archimedische veelvlakken samen met de vijf platonische veelvlakken opgenomen. Het geeft een redelijk overzicht. Maar hoe elk halfregelmatig veelvlak precies in elkaar zit is daaruit misschien lastig op te maken. Daarom passeren ze (met uitzondering van de rhombikuboctaëder) op de volgende bladzijden elk nog eens afzonderlijk de revue (figuren 5 tot en met 16).

Figuur 4

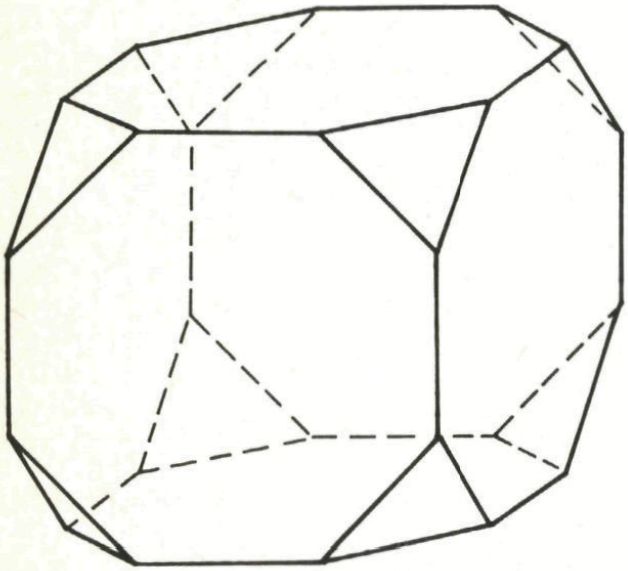




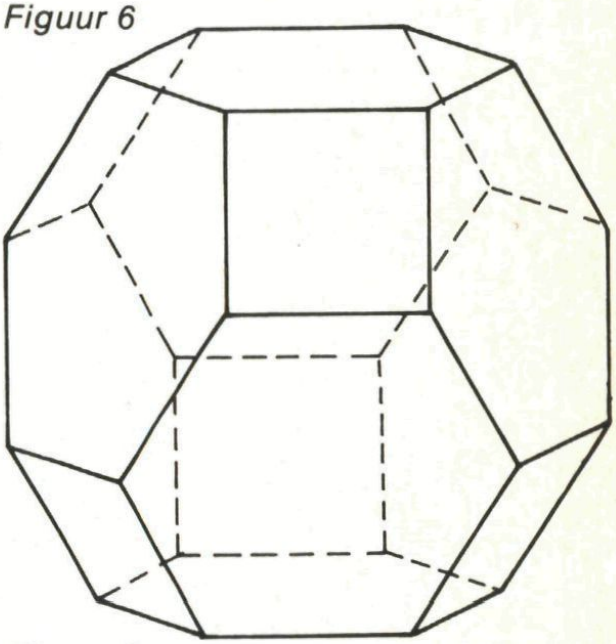
Figuur 5



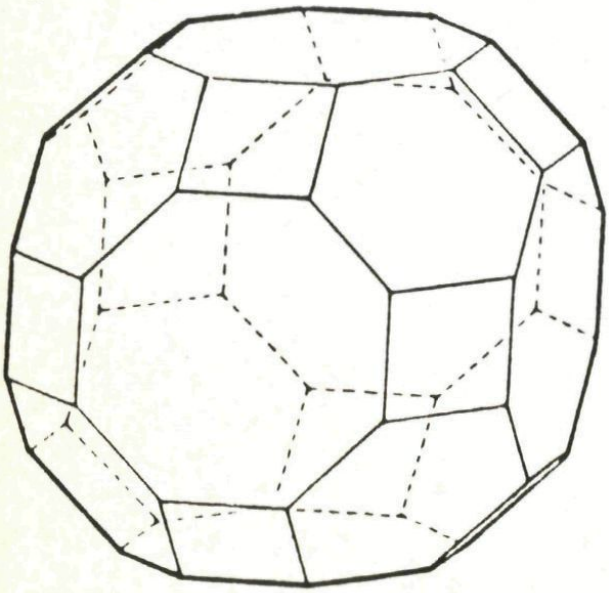
Figuur 6



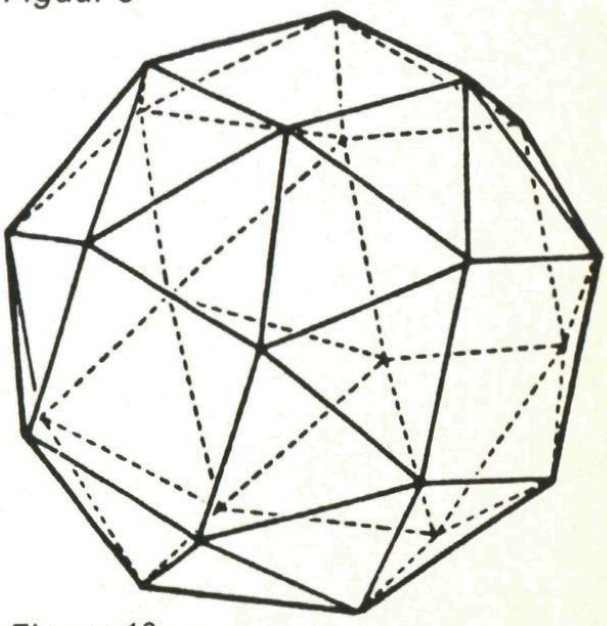
Figuur 7



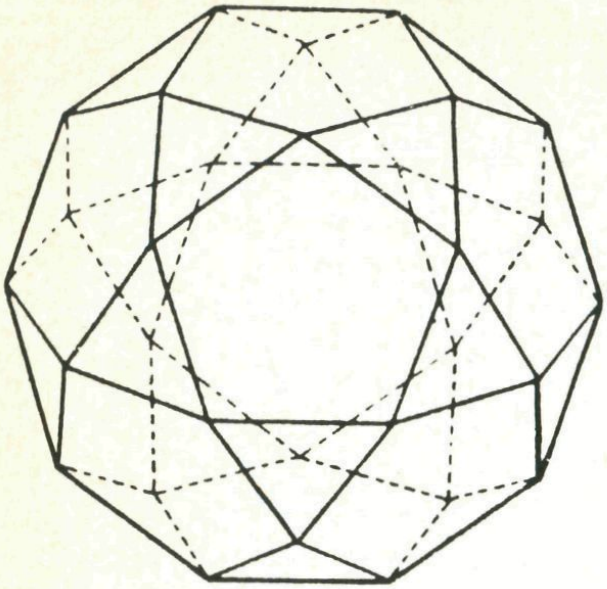
Figuur 8



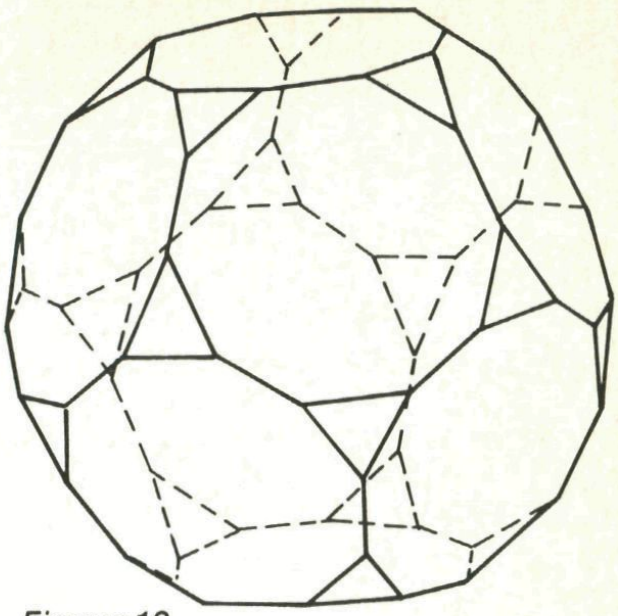
Figuur 9



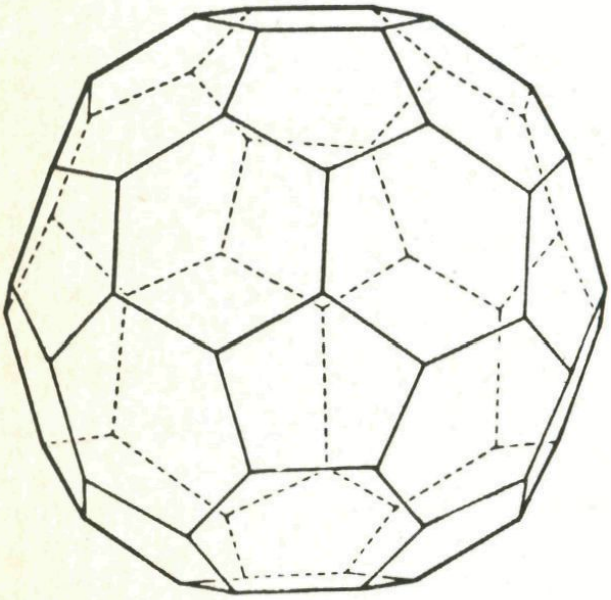
Figuur 10



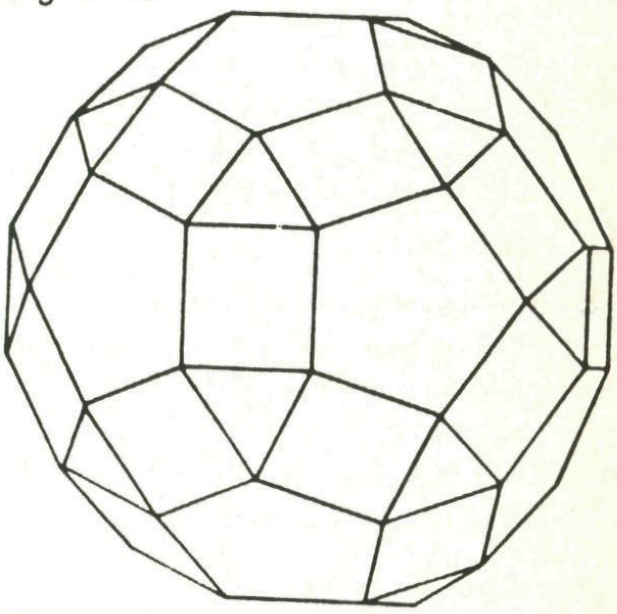
Figuur 11



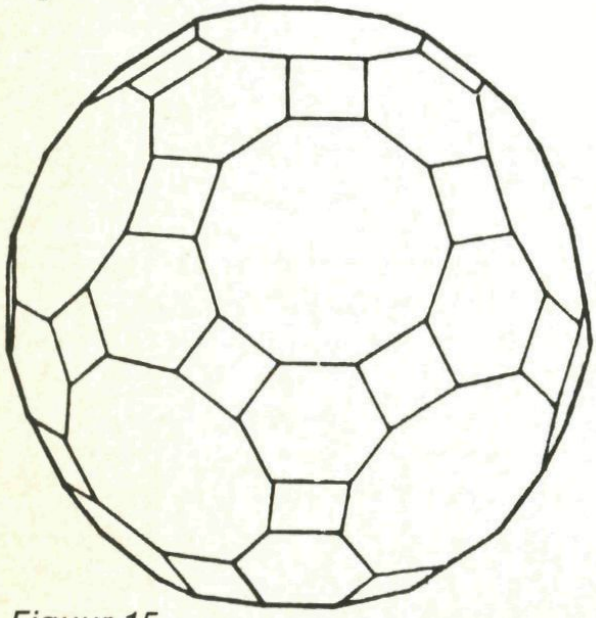
Figuur 12



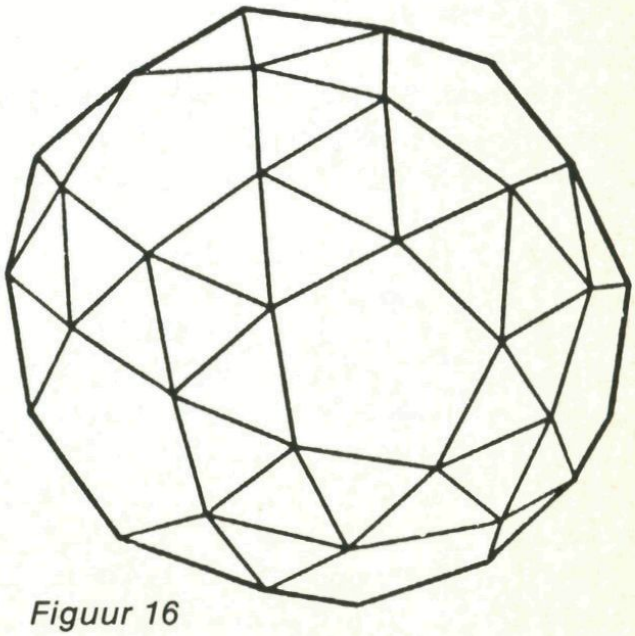
Figuur 13. (Voetbal!)



Figuur 14



Figuur 15



Figuur 16

Figuur	h	r	z	$p_a \times a$	$p_b \times b$	$p_c \times c$
2	24	48	26	1×3	3×4	0
5	12	18	8	1×3	2×6	0
6	12	24	14	2×3	2×4	0
7	24	36	14	1×3	2×8	0
8	24	36	14	1×4	2×6	0
9	48	72	26	1×4	1×6	1×8
10	24	60	38	4×3	1×4	0
11	30	60	32	2×3	2×5	0
12	60	90	32	1×3	2×10	0
13	60	90	32	1×5	2×6	0
14	60	120	62	1×3	2×4	1×5
15	120	180	62	1×4	1×6	1×10
16	60	150	92	4×3	1×5	0

Schematisch overzicht van de dertien halfregelmatige veelvlakken met h *het aantal hoekpunten,* r *het aantal ribben en* z *het aantal zijvlakken. Met* p_a x a, p_b x b *en* p_c x c *wordt het aantal regelmatige veelhoeken (*p_a, p_b *of* p_c*) van elk soort (*a, b *of* c*) aangegeven dat telkens in één hoekpunt samenkomt.*

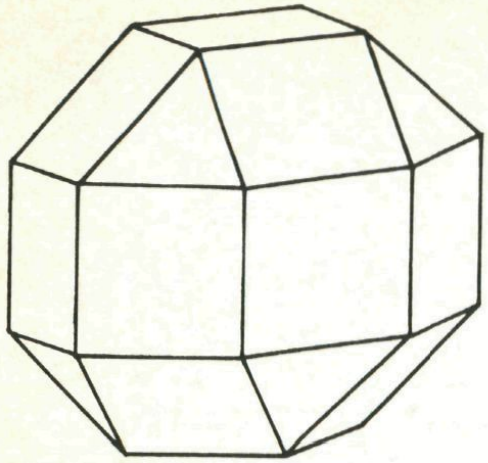
Probeer aan de hand van die figuren het schema na te lopen waarin per veelvlak is opgenomen het aantal hoekpunten, het aantal ribben, het aantal zijvlakken en het aantal veelhoeken van elk soort dat in elk hoekpunt samenkomt.
Merk ook nog even op dat in elk halfregelmatig veelvlak de ribben telkens even lang moeten zijn. □

Een veertiende?

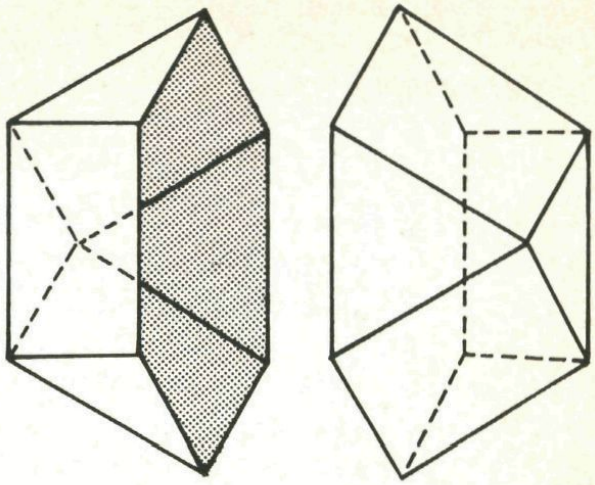
Onder de archimedische veelvlakken neemt uitgerekend dat van de lampekap een bijzondere plaats in. Neem de rhombikuboctaëder (figuur 2, bladzijde 21) nog maar eens voor je. Dit veelvlak bestaat uit twee dakjes die van boven en van onderen tegen een ring van 8 vierkanten zijn geplakt. Elk dakje wordt gevormd door 5 vierkanten en 4 regelmatige driehoeken. Zie je het?

Draai nu in gedachten het bovenste dakje 45° ten opzichte van de rest. Het resultaat wordt figuur 1. Een veelvlak met even veel zijvlakken, hoekpunten en ribben als de rhombikuboctaëder. Dat was ook wel te verwachten. Maar ... het is bovendien halfregelmatig. Het heeft alle eigenschappen die daarvoor nodig zijn. Met name gaat in elk hoekpunt eigenschap 3 op. Rond elk hoekpunt gaande kom je de vierkanten en driehoeken in dezelfde aantallen en in dezelfde volgorde tegen!

Is dit een veertiende halfregelmatig veelvlak? Neen. Het is onmiskenbaar een variant van de rhombikuboctaëder. Het bestaat uit hetzelfde aantal zijvlakken van elk soort, maar iets anders gerangschikt.



Figuur 1



Figuur 2

Isomerie
Dit lijkt op wat in de scheikunde isomerie wordt genoemd. Van eenzelfde stof bestaan verschillende moleculen met eenzelfde aantal atomen van elk soort, maar anders gerangschikt. Daardoor verschillen de eigenschappen van die moleculen soms iets.
Met een paar andere halfregelmatige veelvlakken is een dergelijk kunstje uit te halen. Het levert echter in geen enkel geval weer een halfregelmatig veelvlak op. Zo is bij voorbeeld het halfregelmatige veertienvlak (figuur 6, bladzijde 26) in twee gelijke stukken te splitsen. Draai het ene stuk (figuur 2) 60° ten opzichte van het andere, en plak ze weer tegen elkaar. □

Platvloerse machten

Er is juist één getal van vier cijfers waarvoor geldt

$$A^{B}C^{D} = ABCD$$

In dit uitzonderlijke geval mogen de exponenten omlaag zakken en naast de grondgetallen plaatsnemen.

Typisch een zoekwerkje voor de computer. Schrijf een programma dat *A*, *B*, *C* en *D* bepaalt zodanig dat

A↑B*C↑D = A*10↑3 + B*10↑2 + C*10 + D.

Met gezond verstand, een kladblok en wat doorzettingsvermogen lukt het overigens ook!

Oplossing op bladzijde 32. □

Pythagoras Olympiade

Nieuwe opgaven

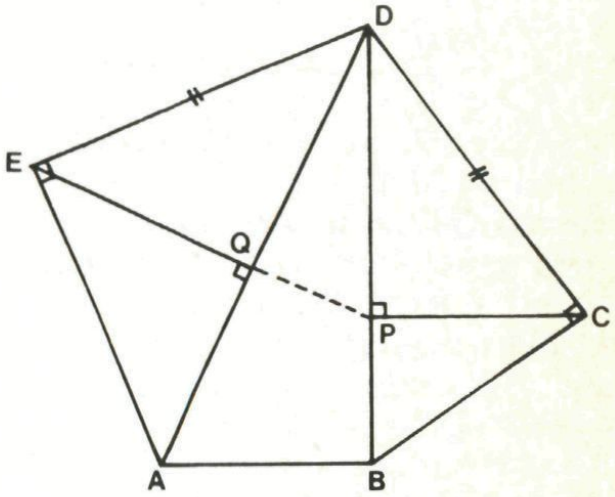
Oplossingen vóór 15 januari insturen naar: *Pythagoras Olympiade, Marinus de Jongstraat 12, 4904 PL OOSTERHOUT (NB).* Vermeld op elk (éénzijdig beschreven) vel je naam, adres, geboortedatum, school, schooltype en klas. Verder moet elke oplossing op een nieuw vel beginnen, want we corrigeren ze afzonderlijk. We bekijken alleen goed leesbare oplossingen die volledig zijn uitgewerkt, met verklarende tekst in goed lopende zinnen. Verdere informatie over de wedstrijd vind je in nummer 1 van deze jaargang op bladzijde 26.

PO 130

Een vijfhoek *ABCDE* (figuur 1) heeft de volgende eigenschappen:

1. $CD = DE$
2. $\angle ABD = \angle BCD = \angle DEA = 90°$.

P en *Q* zijn de voetpunten van de loodlijnen uit respectievelijk *C* en *E* op de diagonalen *BD*, respectievelijk *AD*. Bewijs dat de punten *P*, *Q* en *E* op één lijn liggen.



Figuur 1. Vijfhoek ABCDE.

PO 131

Gegeven zijn twee op elkaar volgende priemgetallen *p* en *q*, beide groter dan 2 (tussen *p* en *q* bevinden zich dus geen andere priemgetallen). Bewijs dat de som $p + q$ geschreven kan worden als het produkt van drie natuurlijke getallen groter dan 1.

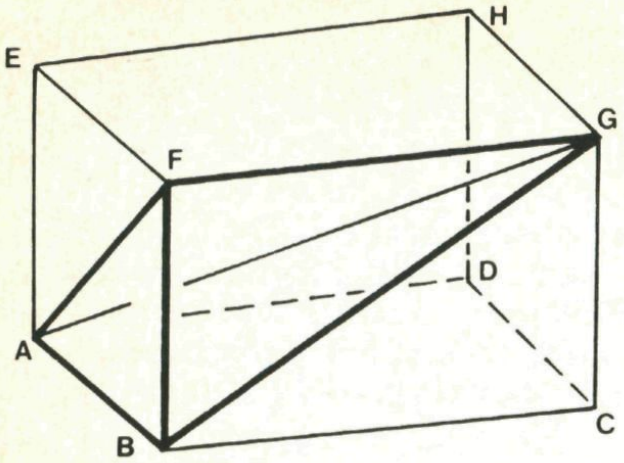
Oplossingen en prijswinnaars van de opgave PO 120

PO 120

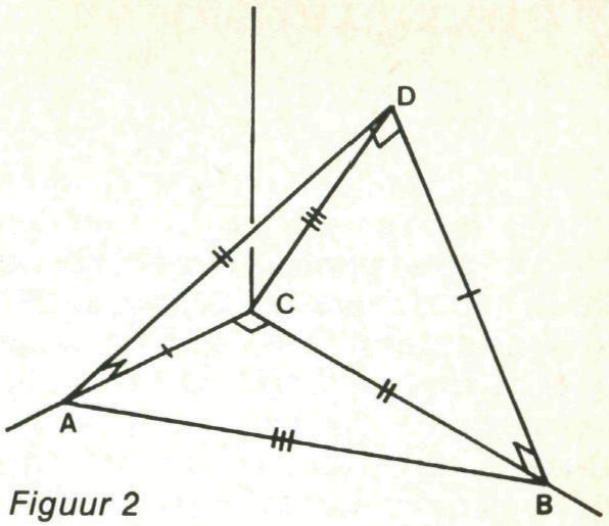
a. Laat zien dat er viervlakken in de ruimte zijn met de eigenschap dat elk zijvlak een rechthoekige driehoek is.
b. Onderzoek of het mogelijk is dat zo'n viervlak vier *congruente* rechthoekige driehoeken als zijvlakken heeft. Motiveer je antwoord!

Oplossing a van *Siebrand Tilma*, 4 vwo, Leeuwarden:

Neem in een willekeurige balk *ABCD.EFGH* het viervlak *ABFG*. Dit voldoet aan de eisen: alle zijvlakken zijn rechthoekige driehoeken (figuur 1). Siebrand laat dit netjes tot in alle details zien, maar onze lezers kunnen dat zelf ook verifiëren. Het aardige van Siebrands voorbeeld is dat je onmiddellijk ziet dat er oneindig veel verschillende mogelijkheden zijn. Je kunt ze bij voorbeeld karakteriseren door



Figuur 1



Figuur 2

de lengte te geven van achtereenvolgens AB, BF en FG, dat wil zeggen de lengte, hoogte en breedte van de balk.

Oplossing b van *Jasper Scholten,* 6 vwo, Heemskerk:
Stel dat $ABCD$ een viervlak is met vier congruente rechthoekige driehoeken als zijvlakken, en stel dat hoek C in driehoek ABC recht is. Omdat de zijvlakken congruent zijn, moet gelden dat $AB = CD$, $BC = DA$, $AC = BD$.
Plaats het viervlak in een rechthoekig coördinatenstelsel met C in de oorsprong, $A = (a, 0, 0)$ en $B = (0, b, 0)$ (figuur 2). Stel dat D de coördinaten (x, y, z) heeft, dan geldt

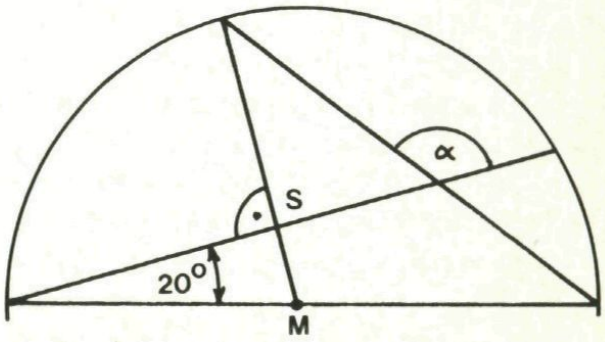
$$CD^2 = AB^2 = a^2 + b^2 = x^2 + y^2 + z^2.$$

Maar omdat de hoeken CAD en CBD recht zijn, geldt ook $x = a$ en $y = b$. Conclusie: $z = 0$, dus de vier hoekpunten liggen in één vlak. Er bestaat dus geen echt ruimtelijk viervlak met vier congruente rechthoekige driehoeken als zijvlakken.

Siebrand en Jasper hadden beide ook de rest van de opgave correct opgelost. Verdere goede oplossingen kwamen van *Timo Gerlach*, 4 vwo, Driebergen, *Erjen Lefeber*, 5 vwo, Zoetermeer, *David Omtzigt,* 5 vwo, Emst, *Martijn Wubs*, 5 vwo, Hoogeveen en *Gijsbert Zwart*, 5 vwo, Geleen. Er was één niet geheel correcte oplossing. Prijswinnaars: *Siebrand Tilma* en *Gijsbert Zwart*. □

Bekijk het even

M is het middelpunt van de halve cirkel. De hoeken bij S zijn recht.
Bereken α. □



Redactioneel

Het is al meer malen aangekondigd, maar nu is het dan zover. In dit nummer alles over magneetstripkaart, PIN-code en chipkaart. Er zijn vier stukjes aan gewijd: 'Je knip op een magneetstrip', 'PIN-code onthouden', 'Zero knowledge proofs' en 'Modulair worteltrekken'. Verder in dit nummer het eerste van twee artikelen over overbodige nullen op postzegels. Het tweede artikel komt in het volgende nummer. Daarin komt tevens de oplossing van de opgave uit het artikel 'Wybertjes in een zeshoek'.

Architectuuraadsels
Onder de titel 'Architectuuraadsels' is bij de boekhandels, aangesloten bij de ICOB, een kalender 1990 (groot formaat en in kleur) te verkrijgen met afbeeldingen van onmogelijke bouwwerken van de Belgische kunstenaar *Jos de Mey*. Aan te bevelen voor liefhebbers van onmogelijke figuren. Kosten: f 12,50.

Rectificatie
Zoals *J. Heijmans* uit Nijmegen terecht opmerkte, zijn in het allerlaatste getal van het artikel 'Reken mee' (Pythagoras 28-5) de laatste drie cijfers weggevallen. Het getal moet niet zijn 201 599 999 798, maar 201 599 999 798 400. □

Platvloerse machten: oplossing

$2^5 \cdot 9^2 = 2592$. Dit unieke getal wordt het getal van Dudeney genoemd. □

Uitgave onder toezicht van de Nederlandse Onderwijscommissie voor Wiskunde.

Lay-out: Klaas Lakeman, Amsterdam.
Tekenwerk: Hans van Kuyk, Amsterdam.
Foto's en andere illustraties: Jack Prince, Den Haag (omslag, blz. 7); Hessel Pot, Woerden (blz. 12, 13, 14, 15); Klaas Lakeman, Amsterdam (blz. 16, 17, 22, 24, 29); B. J. M. Rovers, Eindhoven (blz. 21); Mathematical Models, H. Martyn Cundy & A. P. Rollet, Lomden (blz. 21, 26, 27); Jan van de Craats, Oosterhout (NB) (blz. 30, 31).

druk: koninklijke vermande bv

Pythagoras wiskunde tijdschrift voor jongeren

Redactie: Jan van de Craats, Klaas Lakeman, Hans de Rijk.

Medewerkers: Popke Bakker, Gerard Bäuerle, F. van der Blij, Niels M. Buizert, Hans Lauwerier, Hessel Pot.

Redactiesecretariaat: Klaas Lakeman, Cornelis Krusemanstraat 60II, 1075 NS Amsterdam (NL).

Inhoud jaargang 29, nummer 2

Je knip op een magneetstrip / 1
Klaas Lakeman
PIN-code onthouden / 5
Zero knowledge proofs / 6
Jan van de Craats
Overbodige nullen op postzegels / 12
Hessel Pot
Bekijk het even / 15, 31
Driehoek in vierkant / 16
Klaas Lakeman
Modulair worteltrekken / 18
Jan van de Craats
Lantaarns met opvallende kappen / 21
Klaas Lakeman
De platonische veelvlakken / 22
De archimedische veelvlakken / 24
Een veertiende? / 28
Platvloerse machten / 29, 32
Niels M. Buizert
Pythagoras Olympiade / 30
Jan van de Craats
Redactioneel / 32

Pythagoras verschijnt zesmaal per schooljaar; opgave van abonnementen bij de uitgever (zie onder).
Abonnementen zijn doorlopend, tenzij voor 1 september schriftelijk bij de uitgever is opgezegd.
Bij tussentijdse abonnering ontvangt men ook de reeds verschenen nummers. Betaling per acceptgirokaart.

Tarieven	NLG/BEF
Abonnement Pythagoras	23,—/430
Luchtpost-toeslag	10,—
Inclusief Archimedes	40,—/750
Luchtpost-toeslag	20,—
Losse nummers	5,—/ 90

stichting ivio
Postbus 37, 8200 AA Lelystad (NL.) Tel. 03200-76411
educatieve uitgeverij - instituut voor buitenschools onderwijs - wereldschool - AO-reeks - leerprojecten
Postgiro Nederland: 287934 Postcheck België: 000-0130850-94