platform wiskunde nederland

DIT IS TRIVIAAL

Syllabus Vakantiecursus 2015

Amsterdam, 21 en 22 augustus

Eindhoven, 28 en 29 augustus

platform wiskunde nederland

DIT IS TRIVIAAL

Syllabus Vakantiecursus 2015

Amsterdam, 21 en 22 augustus

Eindhoven, 28 en 29 augustus

Programmacommissie

prof. dr. Frits Beukers (UU)

drs. Joke Blom (CWI)

drs. Swier Garst (PWN)

prof. dr. Wil Schilders (PWN, TU/e)

dr. Jeroen Spandaw (TUD)

dr. Marco Swaen (UvA)

dr. Benne de Weger (TU/e)

prof. dr. Jan Wiegerinck (UvA) (voorzitter)

drs. Bart Zevenhek (Barlaeus)

e-mail: `vakantiecursus@platformwiskunde.nl`

Platform Wiskunde Nederland

Science Park 123, 1098 XG Amsterdam

Telefoon: 020-592 4006

Website: `http://www.platformwiskunde.nl`

Vakantiecursus 2015

De Vakantiecursus Wiskunde voor leraren in de exacte vakken in HAVO, VWO, HBO en andere belangstellenden is een initiatief van de Nederlandse Vereniging van Wiskundeleraren, en wordt georganiseerd door het Platform Wiskunde Nederland. De cursus wordt sinds 1946 jaarlijks gegeven op het Centrum Wiskunde en Informatica te Amsterdam en aan de Technische Universiteit Eindhoven.

Deze cursus wordt mede mogelijk gemaakt door een subsidie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), en een bijdrage van 3TU.AMI, het toegepaste wiskunde-instituut van de 3 Nederlandse technische universiteiten. Organisatie vindt plaats in nauwe samenwerking met het Centrum voor Wiskunde en Informatica (CWI) en de Technische Universiteit Eindhoven (TU/e).

De presentaties van de sprekers zullen zo veel mogelijk beschikbaar komen op de PWN-website:
`http://www.platformwiskunde.nl/onderwijs_vakantiecursus_wiskunde.htm`.

Met dank aan

Ondersteuning PWN: Sjoukje Talsma.
Ondersteuning TU/e: Anita Klooster.

Historie

De eerste vakantiecursus wordt in het jaarverslag 1946 van het Mathematisch Centrum als volgt vermeld:

> *Op 29 en 31 Oct. '46 werd onder auspiciën van het M.C. een druk bezochte en uitstekend geslaagde vacantiecursus gehouden voor wiskundeleeraren in Nederland. Op 29 October stond de wiskunde, op 31 October de didactiek van de wiskunde op de voorgrond. De sprekers waren: Prof.Dr. O. Bottema, "De prismoide", Dr. A. Heyting, "Punten in het oneindige", Mr. J. v. IJzeren, "Abstracte Meetkunde en haar betekenis voor de Schoolmeetkunde.", Dr. H.D. Kloosterman, "Ontbinding in factoren", Dr. G. Wielenga, "Is wiskunde-onderwijs voor alpha's noodzakelijk?", Dr. J. de Groot, "Het scheppend vermogen van den wiskundige" en Dr. N.L.H. Bunt, "Moeilijkheden van leerlingen bij het beginnend onderwijs in de meetkunde".*
>
> *Aan het einde van de vacantiecursus werden diverse zaken besproken die het wiskunde-onderwijs in Nederland betroffen. Een Commissie werd ingesteld, die het M.C. over de verder te organiseren vakantiecursussen van advies zou dienen. Hierin namen zitting een vertegenwoordiger van de Inspecteurs van het V.H. en M.O. benevens vertegenwoordigers van de lerarenverenigingen Wimecos en Liwenagel.*
>
> *Ook werd naar aanleiding van "wenschen" die tijdens de cursus naar voren gekomen waren ingesteld: "een colloquium over moderne Algebra, een dispuut over de didactiek van de wiskunde, beiden hoofdzakelijk bedoeld voor de leeraren uit Amsterdam en omgeving, terwijl tevens vanwege het M.C. een cursus over Getallenleer werd toegezegd te geven door de heeren v.d. Corput en Koksma. (Colloquium, dispuut en cursus zijn in 1947 gestart en verheugen zich in blijvende belangstelling).*

Docenten

Prof. dr. F. Beukers
Universiteit Utrecht, Mathematisch Instituut, Postbus 80010, 3508 TA, Utrecht
e-mail: f.beukers@uu.nl

Dr. A. Blokhuis
Technische Universiteit Eindhoven, Faculteit Wiskunde en Informatica, Postbus 513, 5600 MB, Eindhoven
e-mail: a.blokhuis@tue.nl

Dr. J.H. Brandts
Universiteit van Amsterdam, Korteweg-de Vries Instituut, Postbus 94248, 1090 GE, Amsterdam
e-mail: j.h.brandts@uva.nl

Dr. ir. F.J. Dijksterhuis
Universiteit Twente, MB-STePS, Postbus 217, 7500 AE, Enschede
e-mail: f.j.dijksterhuis@utwente.nl

Dr. A.J. Goddijn
Universiteit Utrecht, Freudenthal Instituut, Princetonplein 5, 3584 CC, Utrecht
e-mail: a.goddijn@uu.nl

Prof. dr. P. Stevenhagen
Universiteit Leiden, Mathematisch Instituut, Postbus 9512, 2300 RA, Leiden
e-mail: psh@math.leidenuniv.nl

Dr. B.M.M. de Weger
Technische Universiteit Eindhoven, Faculteit Wiskunde en Informatica, Postbus 513, 5600 MB, Eindhoven
e-mail: b.m.m.d.weger@tue.nl

Programma

Vrijdag 21 / 28 augustus 2015

15.00–15.30		*Ontvangst, koffie*
15.30–15.35	Wiegerinck	Introductie “Dit is triviaal”
15.35–16.20	Dijksterhuis	Krommen pletten. Kegelsneden in de Gouden Eeuw
16.20–16.45		*Pauze*
16.45–17:30	Blokhuis	Proofs from THE BOOK
17.30–18.30		*Diner*
18.30–19.15	Stevenhagen	De parallelle wereld van de p-adische getallen
19.15–19.45		*Pauze*
19.45–20.30	Goddijn	Intuïtie, inzicht, bewijs

Zaterdag 22 / 29 augustus 2015

10.00-10.30		*Ontvangst, koffie*
10.30-11.15	Beukers	Hoe bewijs je het priemgetaltweeling vermoeden?
11.15-12.00	De Weger	Practicum 1: Hoe snel kunt u vermenigvuldigen?
12.00-13.00		*Lunch*
13.00-13.45	Brandts	Oeps, foutje!
13.45-14.30	De Weger	Practicum 2: Elementair is niet hetzelfde als triviaal
14.30		Afsluiting

Ten geleide

Jan Wiegerinck

Universiteit van Amsterdam

Enig zoeken op Wikipedia leert dat *triviaal* tegenwoordig vooral *alledaags* of *onbeduidend* betekent, maar ook dat de oorspronkelijke betekenis *basaal* of *elementair* is, en dat triviaal binnen de wiskunde in die laatste zin gebruikt wordt. Triviaal is afgeleid van *Trivium*, dat in de middeleeuwen stond voor de drie basisvakken die het eerste deel van de universitaire opleiding besloegen; bij wijze van spreken de bacheloropleiding. Had je dit voltooid, dan was je *baccalaureus* en kon je beginnen aan het *Quadrivium*, wat we nu de masteropleiding zouden noemen, en daarmee de universitaire opleiding bestaande uit de Zeven Vrije Kunsten, afronden. Wiskunde behoorde tot het quadrivium, het was ook in de middeleeuwen al een moeilijk vak!

De vakantiecursus overschrijdt nooit het bachelorniveau, en de cursus van 2015 is in die zin net zo triviaal als de vorige cursussen. Triviaal in meerdere betekenissen zal in deze cursus wel meer op de voorgrond staan.

Fokko Jan Dijksterhuis spreekt over de geboorte van de analytische meetkunde in Nederland in de Gouden Eeuw, in het bijzonder zal hij ingaan op de historische behandeling van kegelsneden. Meer geniaal dan triviaal zijn de ideale *Proofs from the BOOK*; Aart Blokhuis zal er twee bespreken. Het gaat om de oplossing van het derde Hilbert-probleem over het in elkaar overvoeren van veelhoeken van gelijk oppervlak door knippen en plakken, en het Dinitz-probleem over het kleuren van $n \times n$ schaakborden.

Naast de gewone afstand $|a - b|$ tussen rationale getallen a en b, die door completering leidt tot de reële getallen, bestaan er meer exotische, de zogenaamde p-adische afstanden, die aan een sterke vorm van de driehoeksongelijkheid voldoen. Completering leidt hier tot de p-adische getallen. Peter Stevenhagen zal spreken over dit niet-triviale onderwerp dat binnen de moderne getaltheorie een belangrijke plaats inneemt. Met de voordracht van Aad Goddijn keren we weer terug naar de meetkunde. Hij zet analytische en synthetische meetkunde in het VWO tegenover elkaar en laat aan

de hand van oude eindexamenopgaven zien dat beide hun voors en tegens hebben. Frits Beukers zal teruggrijpen op de priemtweelingen die ook vorig jaar aan de orde kwamen. Laat A even zijn, als p en $p+A$ beide priem zijn, spreken we van een A-priempaar. Hoeveel A-priemparen zijn er? Hij gaat in op bewijzen en geschiedenis van dit fascinerende onderwerp. Jan Brandts, tenslotte, gaat ons iets vertellen over de eigenaardigheden van de numerieke analyse. Trivialiteiten als de som van positieve getallen is positief, blijken daar niet zo eenvoudig te liggen!

Ook dit jaar hebben we weer ruimte gemaakt voor een practicum. Benne de Weger verzorgt het practicum over *Hoe snel kunt u vermenigvuldigen* en *Elementair is niet hetzelfde als triviaal.*

Ik hoop dat u ook dit jaar weer veel inspiratie zult opdoen en veel plezier aan de cursus zult beleven!

Inhoudsopgave

1 Krommen pletten. Kegelsneden in de Gouden Eeuw

Fokko Jan Dijksterhuis

In 1646 publiceerde Frans van Schooten de Jongere (1615-1660) zijn eerste boek: *Organica Conicarum Sectionum in Plano Descriptione, tractatus.* Het kan beschouwd worden als een soort sollicitatiebrief waarin hij zijn wiskundige bekwaamheid tentoonspreidde. Van Schooten was kandidaat om zijn vader Frans van Schooten de Oudere (1581-1645) op te volgen als hoogleraar 'Duytsche Mathematique' in Leiden. Dat was een speciaal programma waarin wiskunde werd onderwezen in de landstaal, ten behoeve van vestingbouwers, landmeters en andere mensen uit de praktijk. Niet alleen de taal was aangepast, ook de inhoud van het programma was praktisch georiënteerd. Frans jr. had zijn vader al regelmatig geassisteerd en vervangen en uiteindelijk werd hij inderdaad benoemd als de nieuwe hoogleraar. De Organica was niet in het Nederlands geschreven en ging over een onderwerp dat geen onderdeel van de 'Duytsche Mathematique' was. Desondanks was het een heel passende proeve van bekwaamheid voor deze positie. Van Schooten liet zien dat hij zeer kundig was in de wiskunde, maar bovendien wist hoe je die vertaalde naar de praktijk.

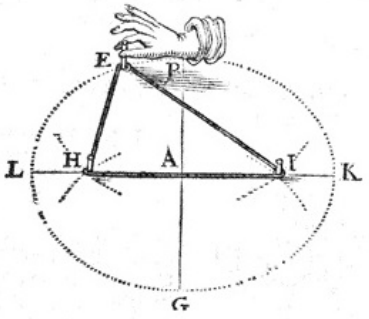
Mechanische beschrijving van kegelsneden in het vlak, zo luidde te titel. Aangevuld met: bruikbaar voor meetkundigen, optici, en in het bijzonder voor gnonomici en mechanici. (Dat laatste wil zeggen: bouwers van zonnewijzers en werktuigen.) Het boek ging over kegelsneden; een klassiek onderwerp uit de wiskunde, maar Van Schooten behandelde het op een nieuwe manier. Gelukkig vertaalde hij zijn boekje een jaar of tien later naar het Nederlands: *Tuych-werckelijcke beschrijving der kegelsneden op een vlack.* Zo kunnen we op ons gemak lezen wat er nieuw aan zijn aanpak was en waarom hij die verkoos. Nadat hij uitgelegd had hoe nuttig het tekenen van parabolen, ellipsen, en hyperbolen was voor zaken als lenzenslijpen, tuinaanleg, ornamenten, en zonnewijzers, vervolgde Van Schooten:

Waerom, nadien het beſchrijven der Kegel-ſneden op een vlack tot ſo veelderhande dingen te pas komt, wat wonder iſſet, dat in't bevorderen van de leering der Kegel-ſneden de treffelijckſte *Mathematici* van oudts af haer ſo hebben bevlijticht, en datter doorgaens, en byſonder in deſe eeuw, een nieuwen aenwas by gekomen is? Doch het geen my wonder geeft, is, dat niemant tot noch toe (dat ick weet) deſe moeyten op hem genomen heeft, namentlijck, datter iemandt gevonden zy, die van de Tuych-werckelijcke beſchrijving der Kegel-ſneden heeft gehandelt, en deſelve in yder voorval betoont.

Met andere woorden: Van Schooten verbaasde zich erover dat het tekenen van kegelsneden in het vlak nog nooit wiskundig behandeld was. De 'mathematici' hielden zich aan de klassieke definitie waarbij een kegelsnede voortgebracht wordt door - zoals het woord al zegt - een kegel met een plat vlak te snijden. Deze definitie ging terug op het hoofdwerk van de kegelsneden, de *Konika* van Apollonius van Perga (c. 262–c. 190 BCE) Deze ruimtelijke constructie speelde geen rol bij het tekenen van ellipsen, hyperbolen, en parabolen in het platte vlak. Dat riep de vraag op in hoeverre die praktische aanpak wiskundig onderbouwd was. Van Schooten wilde in deze lacune voorzien.

Een klassiek voorbeeld van zo'n vlakke voortbrenging is de tuiniersellips. Sla twee pinnen in de grond, leg er een dichtgeknoopt touw omheen, trek een kromme rondom de pinnen met de strakgetrokken lus. Van Schooten liet zien dat deze kromme daadwerkelijk een ellips was die voldeed aan de eigenschappen die Apollonius had afgeleid.

Eyndelijck / dewijlder noch een ander manier in 't gebruyck is / om een Ellipſis op een vlack door behulp van een hoorde of draet rontſom gegeve aſſen te beſchrijven / ſoo heeft 't my goet gedacht die alhier oock by te voegen / op dattet niet noodig zy elders te gaen ſoecken / het gheene tot de volkomme beſchrijving deſer lijn kan begeert worden.



Sy dan den omtreck eener Ellipſis te beſchrijven door behulp van een draet om de gegeve aſſen LK en PG, waer van de grootſte zy LK, en de kleenſte PG. Hier toe ſo zy uyt P of G als centrum in de wijtte LA of AK, de helft der langſte aſſe / beſchreven een circkel-boog / doorſnijdende LK in H en I; en in H en I geſtoockten hebbende twee pennetjens / ſoo laten beyde eynden van de draet aen-een-geknoopt worden / en die om de voorſz pennetjens gelept worden / als hier HEI: want indien men deſe draet met eenige ſtijl in form van een triangel doorgaens eenparich uytſtreckt / en die met de ſtijl rontſom de pennetjens lept / ſo ſal deſelve ſtijl op 't vlack een kromme lijn beſchrijven / als LEPKG, die den omtreck van een Ellipſis zijn ſal. Gelijck blijckt uyt het 52ſte Voorſtel des 3 boecks der Kegel-ſneden Apollonii. Weſhalven ſo men begeert / dat den omtreck der

Met deze tuiniersellips zijn we ook direct bij de kern van Van Schooten's boek. Het is een voorbeeld van een 'tuych-werckelijcke' beschrijving. Er waren ook andere manieren om kegelsneden in het platte vlak voort te brengen, maar die veronderstelden veelal beheersing van de wiskunde. Een voorbeeld is de puntsgewijze constructie. De werktuigelijke voortbrenging daarentegen bestond uit één vloeiende beweging waarvoor alleen het juiste instrument nodig was.

men, hoe qualijck die meeſten tijt gemaeckt zijn: aengeſien die manier het veelvoudig ſoecken van punten en de afgeveerdichtheyt van een geoeffende handt aldaer vereyſcht, gelijck mede, datmen daerenboven, tot een nette uytvoering van het werck, de natuer derſelve linien bekent hebbe. Het welck dan in de Tuych-werckelijcke manier geen plaets en heeft, alſo deſelve de voorſchreve linien, gelijck als van ſelfs, met eene treck terſtont voor oogen ſtelt.

Vorders ſo heeft ons die Tuych-werckelijcke manier boven andre behaegt, dewelcke uyt een aen-een-verknochte beweging zijn oorſpronck neemt, die verwerpende, waer door men deſe linien met een paſſer, tot dien eynde gemaeckt, beſchrijven kan. Nademael men aldaer deſelve linien eerſt beſchreven moet hebben, om, aen de paſſer vaſt gemaeckt zijnde, alleen te konnen dienen tot beſchrijving van diergelicke andre.

In zijn boek introduceerde Van Schooten instrumenten waarmee mensen uit de praktijk zo'n aan-een-verknochte beweging tot stand konden brengen en toonde aan dat de resultaten wiskundig correct waren. Deze combinatie van praktisch vernuft en wiskundige grondigheid was precies wat men van een hoogleraar 'Duytsche Mathematique' mocht verwachten.

De *Konika* van Apollonius kennen een bewogen geschiedenis waarin Leiden een bijzondere rol speelt. In de Renaissance herleefde de belangstelling voor de klassieke wiskunde en voor oorspronkelijke teksten in het bijzonder. Het bestaan van de *Konika* was bekend, maar er waren slechts vier van de acht boeken overgeleverd. Naast het vertalen en redigeren van de oorspronkelijke teksten, maakten wiskundigen zoals Willebrord Snellius (1580-1626) reconstructies van de verloren boeken. Jacob Golius (1596-1667) zorgde in 1627 voor een doorbraak. Hij vond een handschrift met een Arabische vertaling van de *Konika* die drie van de vier verloren boeken bevatte. Het was de zogenaamde Banû Mûsâ editie uit Bagdad, gemaakt door Thâbit ibn Qurra (826-901) in de negende eeuw en beschouwd als de meest originele en complete versie.

Golius was arabist en één van de grondleggers van de oosterse letterkunde in Leiden. Maar hij was ook wiskundige in de breedste zin van het woord en dat combineerde hij met zijn talenkennis. Zo kon hij een tekst als de *Konika* bestuderen. De combinatie van bekwaamheden bracht hem als student in de Arabische wereld, bij diplomatieke missies naar de Maghreb en de Levant. In Aleppo vond hij het Banû Mûsâ manuscript en bracht dat in 1629 terug naar Leiden als onderdeel van een grote collectie waardevolle handschriften. De buit werd vergeleken met de Zilvervloot en het leverde Golius een benoeming op als hoogleraar wiskunde - de leerstoel Arabisch

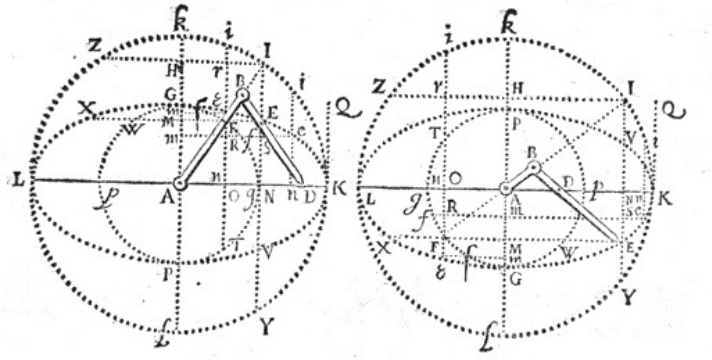
had hij een paar jaar eerder al verworven. Met het Apollonius manuscript zou Golius verder niet zoveel doen: zijn vertaling en editie kwam nooit af en het belandde uiteindelijk in Oxford waar Halley in 1710 een editie publiceerde. Golius wijdde wel zijn leerlingen in in de geheimen van de kegelsneden, waaronder de jonge Frans van Schooten die inzage in het originele handschrift kreeg.

II. HOOFT-STVCK.

Van Ellipſes, dewelcke op een vlack door een aen-een-verknochte beweging om haer aſſen ofte uytterſte diameters beſchreven worden.

ICk kome weder tottet eerſte Inſtrument/ hier boven beſchreven/ dat is/ ick verdencke wederom/ dat in eenig vlack de liniael AB om het vaſte punt A beweecht wort/ en dat aen deſe in B een ander liniael BED vaſt gemaeckt is/ dewelcke om het ſelve in 't voorſz vlack even-eens beweegt han worden. Hier na nemende wyders in BD eenig punt E, naer geballen/ tuſſen B en D, of oock in deſelve buyten D verlengt zijnde; ſoo zy/ als wooren/ BD ghelijck AB: Dan ſeg ick/ ſoo men 't punt D beweegt langs de rechte AD, dat het punt E door die beweeging op 't ſelve vlack den omtreck van een Ellipſis beſchrijven ſal/ wiens centrum is A, en dwerſſche aſſe gelijck aen 't dobbel van AB, BE, en rechte aſſe gelijck aen 't dobbel van DE: Het welck dan te bewijſen is.

Want aengeſien AB beweechlijck geſtelt wort om A, ſoo is openbaer/ indien men eenig punt neemt in AB, of in deſelve verlengt/ waer 't valt/



Van Schooten gaf, zoals we zagen, een geheel eigen, tuigwerkelijke draai aan de kegelsneden. Nogmaals de ellips, maar nu met het instrument van Van Schooten. Het instrument is simpel maar doeltreffend: twee linialen AB en BD scharnieren om elkaar in B; het geheel is vastgemaakt in draaipunt A, terwijl uiteinde D over een rechte lijn door A beweegt. Een punt E op BD (of het verlengde daarvan) beschrijft een ellips. Van Schooten toont dat

netjes aan en op `www.fransvanschooten.nl` staat een GeoGebra appje om ermee te spelen.

Van Schooten leidt allerlei eigenschappen af, stelt ook nog een instrument voor om schuine ellipsen te tekenen. In hoofdstuk komt hij terug bij het oorspronkelijke instrument maar vanuit een andere invalshoek. Het verschil is subtiel maar evident. Het instrument wordt hier in zijn constructie en gebruik besproken. De gedetailleerde wiskundige achtergrond is verdwenen. In de plaats daarvan zijn tastbare latten en ijverige handjes gekomen.

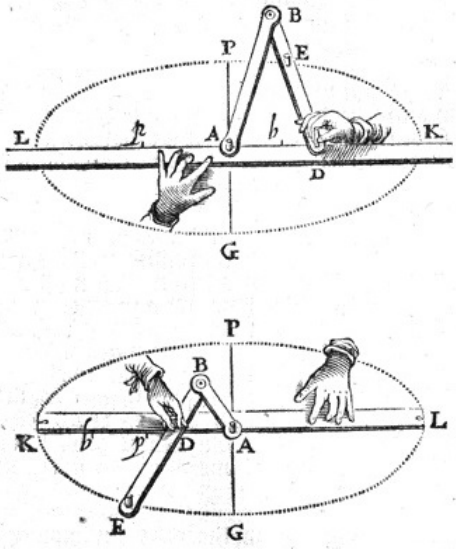
IV. HOOFT-STVCK.

Van de manier om Ellipſes op een vlack te beſchrijven, rontſom gegeve aſſen ofte uytterſte diameters.

NA dat wy in de voorgaende Hooft-ſtucken die dingen verhandelt hebben/ dewelcke als grondt dienen mogen/ waer op de tuych-werckelijcke beſchrijving van een Ellipſis mach gebouwt worden/ ſoo is nu overich dat wy deſelve voetſtappen volgende ons tot het gebruyck bereyden/ betoonende op wat wijz men't geene in deſen deele gemeenlijck voor-geſtelt wort ſal mogen voltrecken.

Wy ſullen dan voor eerſt betoonen/ hoedanig men rontſom gegeve aſſen/ of uytterſte diameters/ Ellipſes op een vlack beſchrijven kan.

Hierom gegeven zijnde op eenig vlack de dwerſche aſſe LK, en GP de rechte t' ſamen gaende met LK, dewelcke malkander in 't centrum A rechthoeckig door-ſnijden: ſoo zy rontſom deſelve op het vlack den omtreck van een Ellipſis te beſchrijven.



Hier toe nemende A p gelijck GA of AP, ſulcx dat p K gelijck zy aen de ſomme of differẽtie van KA en AP (wantter eben-veel is); ſoo zy p K in b gedeelt in 2 gelijcke deelen. Hier na ſo laten genomen worden 2 linialen van koper/ hout/ of eenige andre vaſte ſtoffe/ als AB, BD, die yder ſo lanck zijn als p b of b K; ſoo nochtans/ dat de liniael BD ſo lang zy/ datmen in deſelve van B na D een punt teprikenen kan/ als E, ſulcx dat BE ghelijck zy aen A b. Maer A b

Op deze manier maakt Van Schooten de overstap van meetkundig principe naar praktisch gebruik. En weer terug: analyse en handeling vallen in de Tuych-wercken van Van Schooten volledig samen. Hij geeft een theoretische onderbouwing van tekenpraktijken en een praktische invulling van de analyse van krommen.

Op de achtergrond speelt hier de nieuwe meetkunde van René Descartes: *La Géométrie*, gepubliceerd in 1637 als één van de essays bij zijn *Discours de la Méthode*. Descartes koppelde hierin meetkunde en algebra, waarbij vergelijkingen de oplossing voor meetkundige vraagstukken gaven. Frans van Schooten was als student nauw betrokken bij de totstandkoming van het essay: hij was één van de lezers van de tekst in wording en maakte uiteindelijk de gravures bij *Discours*. Zoals Henk Bos heeft laten zien draaide het in *La Géométrie* om een nieuwe definitie van 'exactheid': welke objecten zijn wiskundig (en welke niet). De klassieke, Euclidische definitie stelt dat mathematisch datgene is wat met passer en liniaal opgelost kan worden. Dat leverde onoplosbare problemen als de kwadratuur van de cirkel en de driedeling van de hoek op. Descartes breidde het begrip exactheid uit: een kromme is mathematisch als hij voortgebracht kan worden door een continue beweging, of een combinatie daarvan. Waar dat bij Descartes abstract-conceptueel blijft, maakt Van Schooten dat concreet met zijn constructies en instrumenten. Een kinematica van de meetkunde.

Met de *Organica* sloeg Van Schooten de brug tussen de 'geometria' van Euclides en Descartes enerzijds en de 'meetkonst' van landmeters en vestingbouwers anderzijds. Het was echter vooral een proeve van zíjn bekwaamheid om les te geven aan de Duytsche Mathematique, geen lesboek. Alleen al vanwege het Latijn was het boekje niet geschikt voor de studenten van de ingenieursschool. Van Schooten trok er een ander type studenten mee: zonen van de gegoede burgerij die belangstelling hadden voor de nieuwe wiskunde en wijsbegeerte van mensen als Descartes. Zoals Christiaan, de tweede zoon van Descartes' beschermheer Constantijn Huygens; Johannes Hudde, een Amsterdams patriciër; en Johan, zoon van het voorname Dordtse geslacht De Witt. In zijn 'privatissimae' bestudeerde Van Schooten met hen de *Géométrie* van Descartes, schreef toelichtingen en aanvullingen, hetgeen uiteindelijk uitmondde in zijn levenswerk: *Geometria, à Renato Des Cartes*. In 1649 gaf hij de eerst editie uit, in 1659–1660 verscheen de tweede, uitgebreid met tal van aanvullingen en annotaties.

Eén van de bijlagen van de *Geometria* was een beschouwing van één van zijn voorname studenten over kegelsneden. In *Elementa Curvarum Linearum* werkte Johan de Witt een analytische behandeling van kegelsneden uit. Hij zette hiermee het werk van zijn leermeester voort, en zette tege-

lijkertijd een stap verder. De platte voortbrenging was voor De Witt de grondslag van de analyse van krommen. Hij had geen last van de bescheidenheid van Van Schooten:

'... achtte ik het volslagen in te gaan tegen de natuurlijke orde, die men in de wiskunde zoveel mogelijk in acht moet nemen, dat men de oorsprong van deze krommen zoekt in een ruimtelijk lichaam en deze vervolgens overbrengt naar het platte vlak.'

Hiermee hadden de klassieken afgedaan en waren de kegelsneden definitief geplet.

2 Proofs from THE BOOK
Aart Blokhuis

2.1 Voorwoord

In 1998 verscheen het boek met bovenstaande titel van Martin Aigner en Günther Ziegler. Het is opgedragen aan de in 1997 overleden beroemde hongaarse wiskundige Paul Erdős van wie het beeld afkomstig is van een BOEK met daarin de ultieme bewijzen van alle belangrijke wiskundige stellingen. Tijdens mijn voordracht zal ik twee hoofdstukken uit dit boek redelijk uitgebreid gaan behandelen.

Hoofdstuk 7 is getiteld "Hilbert's third problem: decomposing polyhedra". In een beroemd geworden voordracht op het internationale congres voor wiskundigen te Parijs in 1900 gaf Hilbert een lijst van 23 problemen die volgens hem belangrijk waren om in de komende eeuw aan te werken. Sommige van die problemen zijn in de loop van de tijd opgelost, anderen staan nog open, maar één ervan werd (een beetje verdacht misschien) binnen een jaar opgelost door zijn student Max Dehn.

Het probleem is als volgt: Elke tweetal veelhoeken in het platte vlak met dezelfde oppervlakte is 'equidecomposable', of 'equidissectable' of 'zerlegungsgleich', dat wil zeggen je kunt de ene met een eindig aantal rechte sneden in stukken verdelen, en die dan zo samenvoegen dat je de tweede krijgt. Bij gebrek aan beter zal ik het woord 'gelijk opdeelbaar' gebruiken. Een leuke puzzel is om een gelijkzijdige driehoek in vier stukken te verdelen, die samen te voegen zijn tot een vierkant. Is iets dergelijks ook waar in hogere dimensies? Het antwoord is nee, als voorbeeld zullen we bewijzen dat een regelmatig viervlak en een kubus met gelijke inhoud niet gelijk opdeelbaar zijn. Dit 'bewijs uit het BOEK' is afkomstig van V.G. Boltianskii en dateert uit 1978.

Een andere plek om over dit probleem te lezen is het (nooit echt gepubliceerde, maar eenvoudig op internet te vinden) populaire en zeer leesbare boek Linear Algebraic Methods in Combinatorics with applications to Geometry and Computer Science van Laszló Babai en Péter Frankl, hoofdstuk

1 paragraaf 3: A Jigsaw Puzzle.

Hoofdstuk 24 is getiteld "The Dinitz Problem". Jeff Dinitz (geboren 1952) is een discreet wiskundige die werkt in Vermont. Zo'n 18 jaar geleden waren we samen met een stel wiskundigen midden in de zomer midden op de dag in het (antieke) olympisch stadion in Delphi en hij stelde mij voor de klassieke afstand 200 meter te rennen. Hoewel hij vier jaar ouder is dan ik, wist hij me toch op de laatste 10 meter nog in te halen.

Zijn probleem is als volgt: Neem een $n \times n$ vierkant, verdeeld in n^2 cellen in n rijen en n kolommen, dus zoiets als een schaakbord. Voor elke cel is een verzameling van n kleuren beschikbaar. Is het mogelijk de cellen (velden) zo te kleuren dat in elke rij en elke kolom de cellen verschillende kleuren hebben. In het speciale geval dat de n beschikbare kleuren voor elk veld hetzelfde zijn wordt eigenlijk gevraagd naar een latijns vierkant van orde n, een $n \times n$-matrix met in elke rij en elke kolom precies de getallen 1 tot en met n, en die zijn zeer eenvoudig te maken.

Dat het algemene probleem ook een oplossing heeft werd pas 15 jaar na dat het in 1978 gesteld was aangetoond door Fred Galvin, met een echt BOEK-bewijs.

2.2 Hilbert's derde probleem

Een leuk probleem voor in de schoolklas is het volgende: Kun je een gelijkzijdige driehoek met een schaar in stukken, met rechte randen, knippen, en met de stukken vervolgens een vierkant (met natuurlijk dezelfde oppervlakte) maken? Er is een mooie oplossing, drie keer knippen, vier stukken, uit 1902 van de Engelse puzzelontwerper H.E. Dudeney.
Hoe zit het in de ruimte? Is het mogelijk een regelmatig viervlak zo te verzagen (weer zo dat de stukken rechte randen hebben), dat uit de stukken een kubus te maken is. (Wiskundig bestaat verzagen uit een eindige reeks operaties van de vorm: breng een vlak aan door een veelvlak, en vervang dit nu door het veelvlak aan de ene kant en het veelvlak aan de andere kant).
Dit is in wezen het derde probleem van Hilbert. Het precieze probleem luidt als volgt:

Sind zwei beliebige Tetraeder mit gleichen Grundflächen und gleichen Höhen

stets zerlegungsgleich oder lassen sie sich mit kongruenten Polyedern zu zerlegungsgleichen Körpern ergänzen?

Een van de redenen voor deze vraag is het ontbreken van een 'eenvoudig' meetkundig bewijs voor Stelling XII.5 uit de elementen van Euclides, dat twee piramiden met gelijke hoogte en met grondvlakken met dezelfde oppervlakte gelijke inhoud hebben (en dat dus deze inhoud gelijk is aan één derde maal basis maal hoogte), iets waar ook Gauss zich al druk over maakte.
In het vlak zijn twee veelhoeken met dezelfde oppervlakte wel altijd gelijk opdeelbaar, dit is de stelling van Bolyai en Gerwien. Hier is Bolyai de hongaarse wiskundige Farkas (of op zijn duits Wolfgang) Bolyai, een goede (correspondentie-)vriend van Gauss en de vader van János Bolyai, die een van de grondleggers is van de hyperbolische meetkunde. Voor de volledigheid citeer ik hier opgave 1.3.3 uit het boek van Babai en Frankl, inclusief de hint:

Bewijs dat twee veelhoeken met dezelfde oppervlakte gelijk opdeelbaar zijn.
Hint: Laat P een veelhoek zijn met oppervlakte 1. Ons doel is het te versnijden en van de stukken een éénheidsvierkant te maken. Begin ermee het te verdelen in driehoeken. Maak vervolgens van elke driehoek een rechthoek. Het lastigste gedeelte is te bewijzen dat rechthoeken (met dezelfde oppervlakte) gelijk opdeelbaar zijn. (Waarom is dit voldoende?) Laat eerst zien dat je een langwerpige rechthoek kunt versnijden tot iets dat meer op een vierkant lijkt, en wel iets waar de zijden binnen een factor 2 van elkaar liggen. Maak het tenslotte af.

2.2.1 De stelling van Dehn

Doel van dit hoofdstuk is het boekbewijs van de volgende stelling: (Max Dehn, 1900)

Een regelmatig viervlak en een kubus (met dezelfde inhoud) zijn niet gelijk opdeelbaar.

We hebben om te beginnen wat lineaire algebra nodig. Met $\mathbf{Q}$ geven we het lichaam van de rationale getallen aan. Voor een willekeurige (eindige) verzameling $M = \{m_1, m_2, \ldots, m_k\}$ van reële getallen definiëren we het $\mathbf{Q}$-opspansel, de verzameling getallen

$$V = V(M) = \{q_1 m_1 + q_2 m_2 + \cdots + q_k m_k \,|\, q_i \in \mathbf{Q}\} \subset \mathbb{R}.$$

V is een vectorruimte over $\mathbf{Q}$: binnen V kunnen we optellen, we kunnen met (rationale) scalars vermenigvuldigen, en alle gebruikelijke regels gelden. Duidelijk is ook dat $\dim(V) \leq k$ want V wordt opgespannen door de 'vectoren' $m_1, m_2, \ldots, m_k$. Een functie $f : V \to \mathbf{Q}$ heet lineair als geldt dat i) $f(a+b) = f(a) + f(b)$ voor alle $a, b \in V$ en ii) $f(qa) = qf(a)$ voor alle $a \in V$ en $q \in \mathbf{Q}$. Voor het lichaam $\mathbf{Q}$ volgt eis ii) overigens uit eis i). Als $u_1, u_2, \ldots, u_d$ een basis is voor een vectorruimte U, en $q_1, q_2, \ldots, q_d$ zijn elementen van $\mathbf{Q}$ dan is er precies één lineaire functie $f : U \to \mathbf{Q}$ met $f(u_i) = q_i$ voor $i = 1, \ldots, k$, met als gevolg dat als u en v lineair onafhankelijk zijn, dan is er een lineaire functie f met $f(u) = 1$ en $f(v) = 0$.
Wat we ook nodig hebben is het volgende feit: Laat $\alpha = \arccos(1/3)$, we zullen zodadelijk zien dat α de hoek is tussen twee zijvlakken van een regelmatig viervlak.

Feit Het getal α/π is irrationaal. Anders gezegd: α en π zijn onafhankelijk (over $\mathbf{Q}$).

Dit kan bewezen worden door gebruik te maken van het feit dat $\cos(nx) = T_n(\cos x)$ voor een polynoom T_n met gehele coëfficiënten en kopcoëfficiënt 2^{n-1}, dus $\cos(2x) = 2\cos^2 x - 1$, $\cos(3x) = 4\cos^3 x - 3\cos x$, $\cos(4x) = 8cos^4x - 8cos^2x + 1$. De T_n zijn de Tsjebysjev polynomen, het handigst kan bovenstaande bewering bewezen worden met behulp van de formule van de Moivre: $(\cos\phi + i\sin\phi)^n = \cos(n\phi) + i\sin(n\phi)$ plus de substitutie $\sin^2\phi = 1 - \cos^2\phi$. Omdat $\cos\alpha = 1/3$ geldt dat $\cos n\alpha$ een rationaal getal wordt waarvan de noemer gelijk is aan 3^n, in het bijzonder is $\cos n\alpha$ dus nooit gelijk aan ± 1 (voor $n > 0$), en dus is $n\alpha$ nooit een veelvoud van π.

Het plan van Dehn is nu als volgt. Bij een veelvlak (zoals een kubus of een tetraeder) definieren we met behulp van een lineaire functie op een geschikte vectorruimte een rationaal getal, de Dehn-invariant. We laten zien dat twee veelvlakken die gelijk opdeelbaar zijn dezelfde Dehn-invariant hebben, tenslotte laten we zien dat een kubus met zijde 1 en een regelmatig viervlak met inhoud 1 verschillende Dehn-invarianten hebben.

We stellen ons om te beginnen voor dat we de kubus en het viervlak allebei kunnen opdelen in veelvlakken $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ voor een of ander getal n. We vormen nu de verzameling $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ van alle hoeken die gemaakt worden door twee (aangrenzende) zijvlakken van een veelvlak uit $\mathcal{P}$. De vectorruimte V zal nu de boven gedefinieerde $V(\Gamma)$ zijn bestaande uit alle getallen van de vorm $q_1\gamma_1 + \cdots + q_m\gamma_m$. Twee van de hoeken in de verzameling Γ zijn $\pi/2$ en α. We gaan nu op $V(\Gamma)$ een lineaire functie f definieren. We stellen om te beginnen $f(2\pi) = 0$, zodat $f(\gamma + 2\pi) = f(\gamma)$

en f dus goed gedefiniëerd is voor hoeken. Uit de lineariteit volgt nu dat $f(q\pi) = 0$ voor elk rationaal getal q en in het bijzonder ook $f(\pi/2) = 0$. Een andere hoek in Γ is natuurlijk α en we kunnen en zullen nu f zo definieren dat $f(\alpha) = 1$. Vervolgens breiden we de definitie van f op één of andere manier uit tot heel $V(\Gamma)$. Nu komt de Dehn-invariant van een veelvlak: Voor elke ribbe r geven we de lengte aan met $L(r)$ en de hoek van de twee zijvlakken op deze ribbe met $\phi(r)$. We definiëren voor een veelvlak P met ribbenverzameling $R(P)$

$$D(P) = \sum_{r \in R(P)} L(r) f(\phi(r)).$$

Merk op dat we voor een kubus Q geldt dat $D(Q) = 0$, omdat alle hoeken gelijk zijn aan $\pi/2$. Voor een regelmatig viervlak T met zijde L krijgen we $D(T) = 6Lf(\alpha) = 6L \neq 0$, dus de Dehn-invarianten zijn inderdaad ongelijk.

Terzijde: Om de hoek tussen twee zijvlakken van een regelmatig viervlak te bepalen kunnen we het eenvoudigst kijken naar de vier hoogtelijnen. Deze staan loodrecht op de zijden, en de hoek tussen twee zijden is gelijk aan de hoek tussen de bijbehorende hoogtelijnen. Kiezen we de oorsprong zo dat deze ligt op het snijpunt van de hoogtelijnen, en de afmeting zo dat de verbindingsvectoren v_i van dit punt met de vier hoekpunten lengte 1 hebben, dan vinden we dat $v_1 + v_2 + v_3 + v_4 = 0$ en nemen we nu het inproduct van deze vector met zichzelf, dan zien we $(v_i, v_i) = 1$ en dus $(v_i, v_j) = -1/3$ als $i \neq j$.

We komen nu tot de essentie van het bewijs: Als we een veelvlak P verzagen met het vlak H en als resultaat stukken P_1 en P_2, dan geldt:

$$D(P) = D(P_1) + D(P_2).$$

Om dit te begrijpen kijken we naar de bijdrage van de verschillende ribben van de onderscheiden veelvlakken. Een ribbe die door H niet doorgesneden wordt en niet in H bevat is blijft ribbe in één van de veelvlakken P_1 en P_2, met dezelfde lengte en dezelfde hoek. Wordt de ribbe echt doorgesneden, dan komt een deel in P_1, een deel in P_2, de hoeken blijven gelijk en de totale lengte van de twee stukken is natuurlijk gelijk aan de oorspronkelijke lengte. Is tenslotte de ribbe gelegen in het vlak H, dan verdeelt H de bijbehorende hoek γ in stukken $\gamma_1 + \gamma_2 = \gamma$, maar omdat $f(\gamma_1 + \gamma_2) = f(\gamma_1) + f(\gamma_2)$ is de bijdrage links en rechts weer gelijk.
Bij het snijden met H ontstaan ook nieuwe ribben, die liggen in een zijvlak van P, en worden ribbe in zowel P_1 als P_2. Voor deze ribben geldt dat de som van de hoeken $\gamma_1 + \gamma_2$ gelijk is aan π en dus $f(\gamma_1) + f(\gamma_2) = 0$ (de lengte is natuurlijk hetzelfde in P_1 en P_2).

2.3 Het vermoeden van Dinitz

Hoofdstuk 24 van HET BOEK is gewijd aan een vermoeden van Dinitz of liever de bevestiging hiervan door Fred Galvin in 1995. Een latijns vierkant is een $n \times n$ matrix met in elke rij en elke kolom een permutatie van de getallen $1, 2, \ldots, n$, hieronder zien we een latijns vierkant van de orde 4:

1	2	3	4
3	1	4	2
2	4	1	3
4	3	2	1

We kunnen een latijns vierkant ook zien als een $n \times n$ schaakbord, waarvan de velden gekleurd zijn met n kleuren en elke kleur één keer voorkomt in elke rij en elke kolom. Latijnse vierkanten van willekeurige orde zijn makkelijk te maken, het is zelfs een sport om uit te rekenen hoeveel er precies zijn bij gegeven n. Voor $n = 1, \ldots, 11$ is het precieze antwoord bekend, een mooie formule is er (waarschijnlijk) niet.
Een gegeneralizeerd latijns vierkant is een $n \times n$ matrix waarin elke rij en kolom n verschillende elementen bevatten, hieronder zien we een gegeneralizeerd vierkant van orde 4:

1	5	3	4
3	1	4	2
2	4	6	3
4	6	2	1

Het vermoeden van Dinitz uit 1978 zegt het volgende: Bij gegeven n^2 verzamelingen S_{ij}, elk met n elementen en met $1 \leq i, j \leq n$ bestaat er een gegeneralizeerd latijns vierkant L, met $L_{ij} \in S_{ij}$, of in termen van kleuringen: Bij een $n \times n$ schaakbord hebben we voor elk veld de keuze uit een verzameling van n mogelijke kleuren (voor dat speciale veld). Dan is er een kleuring van het schaakbord zo dat in elke rij en elke kolom alle velden een andere kleur hebben.
Het boekbewijs is gebaseerd op twee ideeën, de Gale-Shapley stabiele huwelijksstelling, en een idee van Jeanette Jansen (uit Eindhoven), en ook Alon-Tarsi, om een bepaald soort 'oriëntaties' te gebruiken.

2.3.1 De stabiele huwelijksstelling van Gale en Shapley

Beschouw twee (eindige) verzamelingen, mannen: M_i, en vrouwen: V_j. Sommige mannen en vrouwen zijn in principe bereid met elkaar te trouwen, en iedereen wil liever getrouwd zijn dan vrijgezel. Elke man heeft een lineaire ordening van voorkeur op 'zijn' verzameling vrouwen, en omgekeerd heeft elke vrouw zo'n ordening op 'haar' mannen. De stabiele huwelijksstelling zegt dat er een verzameling P van echtparen (M_k, V_l) bestaat, zodanig dat er paar (M_i, V_j) is dat zowel voor M_i als V_j aantrekkelijker is dan wat ze nu hebben.

Bewijs. Man M_1 verlooft zich met zijn favoriete vrouw. M_2 doet hetzelfde, behalve als dit toevallig de verloofde is van M_1, in dat geval kiest deze haar favoriet uit M_1 en M_2. Als M_2 pech heeft, kiest hij de volgende dame op zijn lijstje. M_3 doet ook hetzelfde, enzovoort. Als iedereen geweest is, dan beginnen we opnieuw met de eerste man die nog niet verloofd is. Een vrouw die eenmaal verloofd is blijft verloofd, maar niet noodzakelijk met dezelfde man, na eindige tijd treden er geen veranderingen meer op en kan men gaan trouwen.

2.3.2 Gewone en lijst-kleuringen van grafen

Het vermoeden van Dinitz gaat eigenlijk over (lijst-kant-)kleuringen van grafen. Een graaf $\Gamma = (V, E)$ bestaat uit een verzameling punten V, en een verzameling kanten, puntparen E. Als het paar (a, b) in E zit, dan heten a en b *verbonden* of ook wel *buren* en we schrijven ook $a \sim b$. De graad van een punt is het aantal buren van dit punt. Bij *gerichte graaf* geldt dat de kanten georiënteerd zijn, ze hebben een begin- en een eindpunt, en we schrijven $a \to b$, b heet een uitbuur van a. De uitgraad van a is het aantal uitburen van a.

Een kant-kleuring van Γ is het toekennen van een kleur aan elke kant, zó dat twee kanten die een punt gemeen hebben een verschillende kleur hebben. De volledige bipartiete graaf $K_{n,n}$ is een graaf met $V = R \cup K$, R en K twee disjuncte verzamelingen met n elementen, en $r \sim k$ voor elke $r \in R$ en $k \in K$. Een kant-kleuring van $K_{n,n}$ met n kleuren is hetzelfde als een latijns vierkant met rijverzameling R en kolomverzameling K, en $L(r, k)$ de kleur van de kant (r, k). Een lijst-kant-kleuring van de graaf $\Gamma = (V, E)$, met lijstjes kleuren $C(e)$ voor elke $e \in E$ is het toekennen van een kleur uit $C(e)$ aan kant e, opnieuw zó, dat kanten die een punt gemeen

hebben verschillende kleuren krijgen. Het Dinitz vermoeden zegt dat zo'n kleuring bestaat voor $K_{n,n}$ als $|C(r,k)| = n$ voor elke kant (r,k). Het bewijs van Galvin laat zien dat iets dergelijks geldt voor een willekeurige *elke* bipartiete graaf.

2.3.3 Het oriëntatie-idee

Als we de *punten* willen kleuren van een graaf G, dan willen we dat verbonden punten verschillende kleuren krijgen. Als we de punten willen kleuren van een gerichte graaf, dan willen we dat begin- en eindpunt van een gerichte kant verschillende kleuren krijgen. Het lijkt alsof er geen verschil is, toch maakt het volgende idee gebruik van zo'n oriëntatie van de kanten. Een *coclique* in een (al dan niet gerichte) graaf is een verzameling punten, waartussen geen enkele kant bestaat. We noemen een coclique $\mathcal{C}$ in een gerichte graaf *absorberend*, als voor elk punt $v \notin \mathcal{C}$ er een kant is met beginpunt v en eindpunt in $\mathcal{C}$. Stel dat elke geïnduceerde deelgraaf van G een absorberende coclique bevat, en veronderstel verder dat voor elk punt v een lijst L_v van kleuren beschikbaar is met meer elementen dan de uitgraad van v, dan is het met inductie te bewijzen dat er een bijbehorende lijstkleuring is van de graaf G. Beschouw namelijk een kleur c, en bekijk de deelgraaf H bestaande uit de punten v met $c \in L_v$. Deze deelgraaf heeft een absorberende coclique $\mathcal{C}$. Geef nu de punten in $\mathcal{C}$ kleur c, verwijder $\mathcal{C}$ uit de graaf en kleur c uit alle lijstjes L_v. De nieuwe graaf is kleiner en voldoet nog steeds aan alle eisen.

2.3.4 Galvin's bewijs

Stel B is een bipartiete graaf, met twee soorten punten M_i en V_j, en zekere kanten $e = C_{ij} = \{M_i, V_j\}$. Laat G de lijngraaf zijn van B, punten van G zijn de kanten van B, verbonden als ze een punt van B gemeen hebben. Kant-kleuringen van B corresponderen met punt-kleuringen van G. Stel de punten van G zijn aanvankelijk gekleurd met kleuren, $1, 2, \ldots, \chi$. Wat we laten zien is dat gegeven een lijstje met χ kleuren voor elk punt van G er ook een bijbehorende lijst-punt-kleuring bestaat. We oriënteren de kanten G, met andere woorden, elke kant krijgt een beginpunt en een eindpunt: $C_{ij} \to C_{ij'}$ als $c_{ij} > c_{ij'}$ en $C_{ij} \to C_{i'j}$ als $c_{ij} < c_{i'j}$. Hier staat c_{ij} voor de kleur van C_{ij}. De uitgraad van elk punt is ten hoogste $\chi - 1$,

want de uitburen hebben allemaal een verschillende kleur. Merk op dat de kleuring een lineaire orde definiëert op elke 'rij' $m_i = \{C_{ij} \,|\, V_j \sim M_i\}$, corresponderend met de normale ordening van de kleuren, en ook één op de 'kolom'$v_j = \{C_{i,j} \,|, M_i \sim V_j\}$, corresponderen met de omgekeerde ordening van de kleuren. Wat overblijft om aan te tonen is dat de graaf G, met deze oriëntatie, samen met al zijn deelgrafen een absorberende coclique heeft. Maar dit is precies wat de stabiele huwelijksstelling van Gale en Shapley ons vertelt.

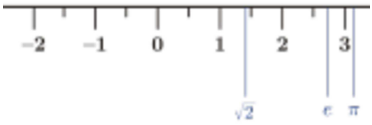
3. DE PARALLELLE WERELD VAN DE p-ADISCHE GETALLEN

Peter Stevenhagen (Universiteit Leiden)

1. Inleiding

Wie op de middelbare school over 'getallen' praat, bedoelt daarmee in den regel *reële* getallen, en, zoals de naamgeving al suggereert, zijn dat getallen die geschikt zijn om de werkelijkheid om ons heen te beschrijven. Intuïtief is tamelijk duidelijk wat reële getallen zijn: men tekent een rechte lijn met daarop een punt genaamd 0, ergens ter rechterzijde een tweede punt op 'eenheidsafstand' genaamd 1, en zegt vervolgens dat de verzameling van alle reële getallen $\mathbf{R}$ *bestaat uit* of *correspondeert met* de punten van de lijn.

Deze ietwat meetkundige definitie gaat terug op de oude Grieken, al hadden die nog geen behoefte aan *negatieve* getallen, die men tegenkomt door van 0 naar links te lopen. Het getal 0 is eveneens een relatief moderne notie, zeker in Europa, waar het pas rond 1200 door Fibonacci geïntroduceerd werd, tezamen met de decimale 'arabische' cijfers. Buiten Europa kwam de 0 al veel eerder voor.



Uitgaande van 0 en 1 komt men door steeds een eenheidsafstand naar rechts te lopen de *natuurlijke getallen* $0, 1, 2, 3, \cdots$ tegen, en wie hier voor gebruik in zijn kasboek of elders de negatieve gehele getallen -1, -2, $-3, \cdots$ aan toevoegt, krijgt binnen $\mathbf{R}$ een *ring* $\mathbf{Z}$ van gehele getallen. De zogenaamde *ring-axioma's* waaraan $\mathbf{Z}$ voldoet [3, §6], betekenen dat men optellen, aftrekken en vermenigvuldigen kan in $\mathbf{Z}$ volgens een aantal bekende regeltjes, die onder meer het speciale karakter van 0 en 1

Typeset by $\mathcal{AMS}$-TEX

met betrekking tot optelling en vermenigvuldiging vastleggen. Het begrip *deling* in $\mathbf{Z}$ geeft aanleiding tot een vergroting van $\mathbf{Z}$: men krijgt het *deellichaam* $\mathbf{Q} \subset \mathbf{R}$ bestaande uit de rationale getallen ('breuken'), die een niet-unieke(!) representatie hebben als quotiënt $\frac{a}{b}$ van gehele getallen a en $b \neq 0$. In een lichaam gelden weer alle ring-axioma's, en men kan bovendien onbeperkt delen door elementen verschillend van 0.

Aan rationale getallen heeft men in het dagelijks leven genoeg om alles te kunnen tellen en meten, maar voor een mooie *theorie* is meer nodig. De Grieken hadden een begrip van (met passer en liniaal) *construeerbare* reële getallen, uitgaande van de 0 en de 1 op de getallenlijn, en algemener een begrip van construeerbare punten in het vlak, uitgaande van een gegeven verzameling van punten in het vlak. Zie bijvoorbeeld [3, §25].

Opgave 1. Definieer exact wanneer een reëel getal construeerbaar is, en laat zien dat rationale getallen construeerbaar zijn. *Laat ook zien dat de construeerbare getallen een deellichaam van $\mathbf{R}$ vormen.

De Grieken wisten heel goed dat er construeerbare getallen bestaan die *niet-rationaal* zijn, zoals de lengte $\sqrt{2}$ van de diagonaal van een eenheidsvierkant. Voor een getal als π, dat als omtrek van een cirkel met eenheidsdiameter zeer 'reëel' oogt, bleef meer dan twee millennia lang onduidelijk of het construeerbaar was. Pas in 1882 bewees Lindemann dat π een *transcendent* getal is, en de sinds de Grieken gezochte *kwadratuur van de cirkel* daardoor onmogelijk.

In de begintijd van de moderne wiskunde, in de 17e en 18e eeuw, stond de calculus en infinitesimaalrekening centraal, en maakten wiskundigen veelvuldig gebruik van de intuïtief duidelijke eigenschap van de getallenlijn dat er 'geen gaatjes in zitten'. Hieruit volgen stellingen als de *tussenwaardestelling* voor continue functies, en bekende criteria voor de convergentie van rijen en reeksen. Pas in de negentiende eeuw begon men zich zorgen te maken over een 'echte definitie' van de reële getallen, die dergelijke feiten van een solide fundament kunnen voorzien.

Het dichtstoppen van de 'gaatjes' die het lichaam $\mathbf{Q}$ ongeschikt maken als basisobject in de calculus kan op een aantal manieren geschieden. Het bekendst zijn de definitie van $\mathbf{R}$ uit $\mathbf{Q}$ door middel van *Dedekindsneden*, waarin een reëel getal α in essentie gedefiniëerd wordt als de verzameling van rationale getallen kleiner dan α, en de definitie door middel van *Cauchy-rijtjes*, waarin de reële getallen verschijnen als *limieten* van (rijtjes van) rationale getallen.

In de 20e eeuw realiseerde men zich dat er ook andere, meer *aritmetische* manieren zijn om de gaatjes in het lichaam $\mathbf{Q}$ dicht te stoppen. Die leiden tot de lichamen $\mathbf{Q}_p$ van p-adische getallen, die in sommige opzichten op $\mathbf{R}$ lijken, maar in andere opzichten zich anders gedragen – al kan men

bepaald niet zeggen dat die andere gedragingen altijd 'moeilijker' zijn. Ze zijn het het thema van deze inleidende tekst.

2. Congruenties

In de getaltheorie probeert men vaak vergelijkingen – preciezer: polynomiale vergelijkingen met gehele coëfficiënten, ook wel *Diophantische vergelijkingen* genoemd – op te lossen in gehele of rationale getallen. Men kan hierbij denken aan de vergelijking

$$x^2 + y^2 = z^2,$$

waarvan de geheeltallige oplossingen vanwege hun verband met de stelling van Pythagoras *Pythagoreïsche tripels* worden genoemd, of algemener aan die van de Fermatvergelijking

$$x^n + y^n = z^n,$$

waarvan we sinds het bewijs van Wiles uit 1995 weten dat ze voor $n \geq 3$ allemaal 'triviaal' zijn in de zin dat steeds $xyz = 0$ geldt. In termen van rationale getallen $X = \frac{x}{z}$ en $Y = \frac{y}{z}$ kan men de vragen over geheeltallige oplossingen ook 'meetkundiger' formuleren, in termen van het bestaan van punten met rationale coördinaten op de vlakke krommen gegeven door de vergelijkingen

$$X^2 + Y^2 = 1 \qquad \text{en} \qquad X^n + Y^n = 1.$$

Merk op dat dezelfde vraag voor punten op deze krommen met reële coördinaten een stuk minder interessant is, juist omdat $\mathbf{R}$ geen gaatjes heeft, en de reële punten de hele kromme 'vullen'.

Om te kijken of een algemene 'polynomiale' vergelijking met gehele coëfficiënten oplossingen heeft, is het vaak nuttig om te kijken of zo'n vergelijking oplossingen *modulo* n heeft voor geschikt gekozen n. Dat geeft informatie over mogelijke oplossingen, en laat ook vaak zien dat er helemaal geen oplossingen kunnen bestaan.

Voorbeeld. *Bepaal alle geheeltallige oplossingen van de vergelijking*

$$3x^2 + 2 = y^2.$$

Wie meetkundig ingesteld is, herkent in deze vergelijking een hyperbool H in het platte vlak.

Opgave 2. Teken in het platte vlak $\mathbf{R}^2$ de kromme H met vergelijking $3x^2 + 2 = y^2$.

Anders dan een cirkel of de Fermatkromme $X^n + Y^n = 1$ met even exponent n heeft H *reële* punten die willekeurig ver van de oorsprong liggen, dus het is zeer wel denkbaar dat er oneindig veel punten met geheeltallige coördinaten op zo'n kromme liggen. Het 'reële plaatje' brengt in zo'n geval de oplossing niet direct dichterbij.

Rekenen modulo $n = 2$, wat niets anders is dan kijken naar de *pariteit* van x en y in een mogelijke oplossing, geeft een eenvoudige restrictie: getallen x en y die aan $3x^2 + 2 = y^2$ voldoen zijn óf beide even, óf beide oneven. Schrijven we de vergelijking als $2 = y^2 - 3x^2$, dan wordt duidelijk dat x en y niet beide even kunnen zijn. Immers, omdat het kwadraat van een even getal deelbaar is door 4, is voor x en y even het getal $y^2 - 3x^2$ deelbaar door 4, en dus niet gelijk aan 2: een tegenspraak 'modulo 4'. We blijven zitten met de mogelijkheid dat x en y allebei oneven zijn. In dit geval kijken we modulo 8, de volgende macht van 2, en merken op dat kwadraten van *oneven* getallen altijd in de *restklasse* 1 modulo 8 liggen, hetgeen betekent dat ze een achtvoud plus 1 zijn:

$$(1 + 2k)^2 = 1 + 4(k + k^2) = 1 + 8\frac{k(k+1)}{2}.$$

Dit betekent dat voor oneven x en y het linkerlid van de vergelijking $3x^2 + 2 = y^2$ een achtvoud plus 5 is, terwijl het rechterlid een achtvoud plus 1 is. In het bijzonder kan dus geen gelijkheid gelden: $5 \not\equiv 1 \bmod 8$. We concluderen dat de vergelijking geen geheeltallige oplossingen kan hebben, omdat dit 'modulo een voldoend hoge macht van 2' niet mogelijk is.

Opgave 3. Leid dit resultaat nogmaals af door te laten zien dat de vergelijking $3x^2+2 = y^2$ geen oplossingen heeft modulo 3.

Opgave 4. Laat zien dat de vergelijking $3x^2 + 2 = y^2$ ook geen oplossingen heeft in *rationale* getallen x en y.

Opgave 5. Laat zien dat de vergelijking $55x^3 + 3 = y^3$ geen geheeltallige oplossingen heeft.
[Hint: kijk naar restklassen modulo 7 of 9.]

***Opgave 6.** Laat zien dat de vergelijking $x^2 - 1 = 2y^2$ een hyperbool in het platte vlak beschrijft, en dat er oneindig veel punten met geheeltallige coördinaten op deze hyperbool liggen.

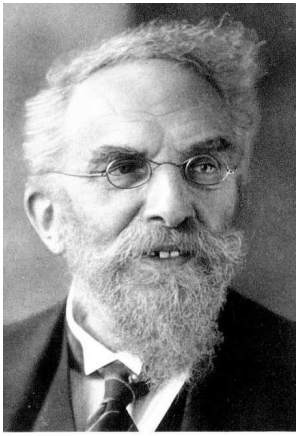
Bij het rekenen modulo n kan men de berekening altijd reduceren tot berekeningen modulo de *priemmachten* die men tegenkomt in de ontbinding van n. Immers, een getal modulo $12 = 2^2 \cdot 3$ weten is hetzelfde als het

modulo 4 en modulo 3 weten. In zijn algemeenheid staat deze wijsheid bekend als de *Chinese reststelling*, waarbij de naam aangeeft dat de oorsprong van de stelling vele eeuwen terug gezocht moet worden. We gaan hier nu niet verder op de precieze formulering in, maar noemen de stelling ter rechtvaardiging van het feit dat we voorlopig congruenties modulo machten van een priemgetal p zullen bekijken. De resulterende notie is die van een *p-adisch getal*.

Opgave 7. Geef een wiskundig correcte formulering van de Chinese reststelling, en probeer te achterhalen hoe oud de stelling is.

3. Reële getallen – herhaling

Het idee dat men geheeltallige oplossingen van vergelijkingen, zo zij al bestaan, kan 'benaderen' door ze modulo steeds hogere machten van één of meer priemgetallen p uit te rekenen is op zich niet zo verrassend, en kan al ver terug in de wiskundige literatuur getraceerd worden. Aan een systematische introductie van dit p-adische gezichtspunt is de naam verbonden van de Duitse wiskundige Kurt Hensel (1861–1941). Zijn leerling Helmut Hasse (1898–1971), die in de dertiger jaren van de vorige eeuw tot de wereldtop in de getaltheorie behoorde, droeg in belangrijke mate bij aan de popularisering van dit gezichtspunt.



Kurt Hensel

De p-adische benadering van oplossingen van Diophantische vergelijkingen doet in veel opzichten denken aan hun bekendere benadering door 'gewone' reële getallen, die we ter wille van de analogie hier eerst nog even bekijken.

Een reëel getal bestaat uit een geheel deel, zijn *entier*, en een een 'rest' die in het halfopen interval $[0,1)$ van getallen x met $0 \leq x < 1$ ligt. Voor het gehele deel is er de bekende *decimale representatie* met behulp van de cijfers 0 tot en met 9, waarbij men een getal als 120345 interpreteert als

$$120345 = 1 \cdot 10^5 + 2 \cdot 10^4 + 0 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 5.$$

Merk op dat de 0, die men niet aantreft bij de Romeinen met hun 'lettercijfers' M, C, X, I voor de laagste machten van 10, een essentiële rol speelt in een dergelijk *positiestelsel*, en dat 'dezelfde' decimale cijfers 'naar links toe' steeds grotere machten van 10 representeren.

Voor het *exact* beschrijven van een reëel getal x in het halfopen interval $[0,1)$ door middel van een *oneindige* decimale ontwikkeling deelt men het interval $[0,1)$ op in tien disjuncte halfopen intervallen van gelijke lengte,

$$[0,1) = [0,\tfrac{1}{10}) \cup [\tfrac{1}{10},\tfrac{2}{10}) \cup [\tfrac{2}{10},\tfrac{3}{10}) \cup [\tfrac{3}{10},\tfrac{4}{10}) \cup \ldots \cup [\tfrac{8}{10},\tfrac{9}{10}) \cup [\tfrac{9}{10},1),$$

die men op de voor de hand liggende manier met de cijfers 0 tot en met 9 labelt. Het *eerste* cijfer in de decimale expansie van x geeft nu het halfopen interval aan waarin x ligt. Dit halfopen interval, dat lengte $\frac{1}{10}$ heeft, verdeelt men op soortgelijke wijze in tien halfopen intervallen van lengte $\frac{1}{100}$, gelabeld met de cijfers 0 tot en met 9, en het tweede cijfer in de decimale expansie van x geeft aan in welk deelinterval x gevonden kan worden. Zo verder gaande kan men uit de eerste n decimalen van de expansie

$$x = 0, c_1 c_2 c_3 c_4 c_5 \ldots$$

van x met cijfers $c_i \in \{0,1,2,3,\ldots,9\}$ een halfopen interval van lengte $\frac{1}{10^n}$ aflezen waarin n ligt. De intuïtief duidelijke gedachte is nu dat de volledige decimale expansie van x het reële getal $x \in [0,1)$ *uniek* vastlegt, in de zin dat het x 'gegeven wordt' door de oneindige som

$$x = \sum_{k=1}^{\infty} \frac{c_k}{10^k},$$

en algemener dat een decimaal gerepresenteerd reëel getal

$$c_{-m} c_{-m+1} c_{-m+2} \ldots c_{-1} c_0, c_1 c_2 c_3 c_4 c_5 \ldots$$

de 'waarde' $\sum_{k=-m}^{\infty} c_k \cdot 10^{-k}$ heeft.

Wiskundigen weten dat het wat voeten in aarde heeft om met enige strengheid te zeggen wat hier precies mee bedoeld wordt, maar ook de pragmatisch ingestelde gebruiker van reële getallen realiseert zich waarschijnlijk

direct dat er geen computer is die daadwerkelijk met zulke oneindige expansies uit de voeten kan. In de praktijk behelpt men zich daarom altijd met *eindige* expansies $x \approx \sum_{k=1}^{N} \frac{c_k}{10^k}$, en werkt dan 'nauwkeurig tot op N decimalen'. Het bewaren van een gewenste nauwkeurigheid, die aanleiding geeft tot het begrip *significante cijfers* bij reële getallen en het onderwerp is van de *foutenanalyse* bij numerieke berekeningen door computers, laat zien dat het in de praktijk nog niet zo eenvoudig is om reële getallen in termen van decimale expansies daadwerkelijk met de realiteit verband te laten houden.

Het is een bekend feit dat de meeste rationale getallen, zoals de oplossing

$$\tfrac{1}{3} = 0,333333333333333333\ldots$$

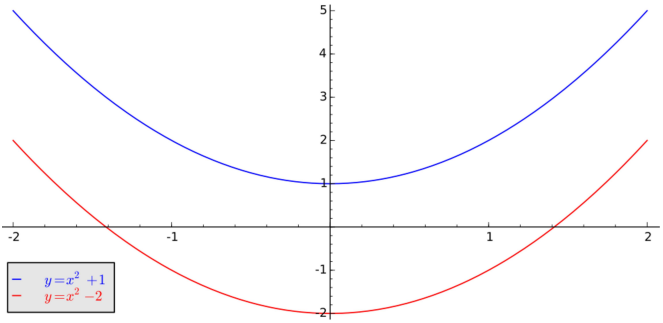
van de allereenvoudigste Diophantische vergelijking $3x = 1$, een *oneindige* decimale expansie hebben. Vermenigvuldigt men in bovenstaand voorbeeld met 3, om in de voetsporen van talloze handrekenmachientjes te komen tot de identiteit

$$1 = 0,999999999999999999\ldots,$$

dan ontdekt men nog dat de boven afgeleide manier om reële getallen aan een decimale expansie te koppelen niet de enig mogelijke is. Een *eindige* expansie, die $c_k = 0$ heeft voor alle voldoend grote k, kan men oneindig maken door het laatste niet-nul cijfer in de expansie met 1 te verlagen, en alle volgende cijfers gelijk aan 9 te nemen.

Opgave 8. Laat zien dat een rationaal getal een decimale expansie heeft die (uiteindelijk) *periodiek* is. Is omgekeerd ieder reëel getal met een periodieke decimale expansie rationaal?

De bestaansreden van reële getallen is niet dat ze een decimale expansie hebben, maar hun eigenschap dat ze de 'gaten' opvullen die worden opengelaten door de rationale getallen op de reële rechte. Wie een plaatje tekent van de parabool die de functie $y = x^2 - 2$ beschrijft, ziet direct dat die parabool de x-as doorsnijdt in de intervallen $(-2, -1)$ en $(1, 2)$. Er bestaat *dus* een reëel getal $\sqrt{2} \in (1, 2)$, dat net als zijn tegengestelde $-\sqrt{2} \in (-2, -1)$ de eigenschap heeft, dat zijn kwadraat gelijk is aan 2. Het plaatje voor de parabool behorende bij $y = x^2 + 1$ laat even overtuigend zien dat er *geen* reëel getal $\sqrt{-1}$ met kwadraat -1 bestaat.



Het is niet moeilijk om te bewijzen dat het getal $\sqrt{2}$ niet rationaal is (opgave!), maar men kan het wel met rationale getallen willekeurig goed benaderen, bijvoorbeeld door de oneindige (niet-periodieke!) expansie

$$\sqrt{2} = 1,41421356237309504880168872420969807856967187537694807 3\ldots$$

na eindig veel decimalen af te kappen. Het snel *vinden* van zo'n decimale expansie is een probleem waar we zometeen nog op terugkomen – er zijn betere methoden dan het naïef kwadrateren van waarden in de buurt van $\sqrt{2}$ om onder- en bovengrenzen te krijgen. Voor $\sqrt{-1}$ kunnen we ons die moeite besparen – dat is geen reëel getal.

4. Spelen met 5-adische getallen

Hoewel de vergelijkingen $x^2 - 2 = 0$ en $x^2 + 1 = 0$ geen oplossingen in $\mathbf{Q}$ hebben, is het niettemin interessant om te kijken of ze oplossingen hebben modulo de *machten* van een priemgetal. Modulo machten van 2 is er in dit geval niet veel te beleven.

Opgave 9. Laat zien dat $x^2 - 2 = 0$ en $x^2 + 1 = 0$ oplosbaar zijn modulo 2^k voor $k = 1$, maar niet voor enige andere waarde $k > 1$.

Modulo machten van het priemgetal 5 gebeurt er echter wel wat aardigs. Door de vijf mogelijke restklassen $0, \pm 1, \pm 2$ die een geheel getal modulo 5 kan hebben te kwadrateren, zien we dat 0, 1 en -1 kwadraten zijn modulo 5, maar 2 en -2 niet. Modulo 5 bestaat er dus *geen* wortel uit 2, maar zijn er wel twee wortels ± 2 uit -1. Kijken we modulo $5^2 = 25$, dan kunnen we de wortels $(\pm 2 \bmod 5)$ uit $(-1 \bmod 5)$ 'verfijnen' tot de wortels

$$\pm 7 \bmod 25 = \pm(2 + 1 \cdot 5) \bmod 25$$

uit $(-1 \bmod 25)$. Immers, er geldt $(\pm 7)^2 + 1 = 50 \equiv 0 \bmod 25$. Het is altijd mogelijk om een dergelijke 5-*adische verfijning* van een oplossing x_k van de vergelijking $x^2 + 1 = 0$ modulo 5^k tot een oplossing $x_{k+1} = x_k + c \cdot 5^k$ modulo 5^{k+1} te vinden, door het getal c geschikt te kiezen.

Lemma. *Laat $x_k \in \mathbf{Z}$ voldoen aan $x_k^2 \equiv -1 \bmod 5^k$ voor zekere $k \geq 1$. Dan bestaat er een 5-adische verfijning $x_{k+1} = x_k + c \cdot 5^k$ die voldoet aan $x_{k+1}^2 \equiv -1 \bmod 5^{k+1}$.*

Bewijs. Er geldt $x_k^2 = -1 + a \cdot 5^k$ voor zekere $a \in \mathbf{Z}$, en we zoeken een getal $x_{k+1} = x_k + c \cdot 5^k$ waarvoor

$$x_{k+1}^2 + 1 = x_k^2 + 1 + 2c \cdot 5^k + 5^{2k} = (a + 2c) \cdot 5^k + 5^{2k}$$

deelbaar is door 5^{k+1}. Kies hiertoe $c = 2a$, dan deelt 5 de factor $a+2c = 5a$ en is de hele uitdrukking deelbaar door 5^{k+1}. $\square$

Omdat alleen de restklasse modulo 5 van het getal c in het voorgaande lemma van belang is – we willen x_{k+1} immers slechts weten modulo 5^{k+1} – kunnen we de '5-adische cijfers' c die we door toepassen van het lemma voor $k = 1, 2, 3, \ldots$ tegenkomen steeds kiezen uit een vaste verzameling zoals $\{0, 1, 2, 3, 4\}$. Uitgaande van $x_1 = 2$ krijgen we dan na 15 stappen

$$\begin{aligned} x_{16} = 2 + 5 + 2 \cdot 5^2 + 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + 2 \cdot 5^6 + 3 \cdot 5^7 \\ + 3 \cdot 5^9 + 2 \cdot 5^{10} + 2 \cdot 5^{11} + 4 \cdot 5^{13} + 5^{14} + 3 \cdot 5^{15}. \end{aligned}$$

Decimaal hebben we $x_{16} = 102662389557$, en uit de factorisatie

$$x_{16}^2 + 1 = 2 \cdot 5^{16} \cdot 34536050621$$

zien we dat x_{16} inderdaad modulo 5^{16} een wortel uit -1 is. De volgende waarde $x_{17} = x_{16} + 2 \cdot 5^{16} = 407838170807$ ziet er decimaal weer heel anders uit, maar in *5-adische notatie* met cijfers 0, 1, 2, 3, 4 hebben we heel eenvoudig

$$x_{16} \overset{5}{=} 2121342303220413. \qquad \text{en} \qquad x_{17} \overset{5}{=} 21213423032204132.$$

Geïnspireerd door de decimale ontwikkeling van reële getallen willen we nu de eindige 5-adische expansies $x_n \overset{5}{=} c_0 c_1 c_2 \ldots c_n = \sum_{k=0}^{n} 5^n$ 'uitbreiden' tot oneindig voortlopende expansies, en algemener een 5-adisch getal genoteerd als

$$x \overset{5}{=} c_{-m} c_{-m+1} c_{-m+2} \ldots c_{-1}, c_0 c_1 c_2 c_3 c_4 c_5 \ldots$$

de 'waarde' $\sum_{k=-m}^{\infty} c_k \cdot 5^k$ geven. Voor onze rij $(x_n)_n$ van benaderende wortels van -1 is de limiet een 5-adisch getal met een oneindige 5-adische

expansie, en daarvoor geldt natuurlijk, afgezien van de uniciteit tot op een factor -1 van het $\sqrt{}$-symbool,

$$\lim_{n\to\infty} x_n = \sqrt{-1}.$$

Net als in het geval van decimale expansies is er ook hier enig zuiver wiskundig werk te doen om een en ander exact te maken, en hier gaan we nog wat nader op in. De praktisch ingestelde p-adicus kan echter gewoon aan de slag met het aldus ontstane *lichaam* $\mathbf{Q}_5$ van 5-adische getallen, dat kennelijk, anders dan $\mathbf{R}$, wel een wortel uit -1 maar geen wortel uit 2 bevat.

Opgave 10. Laat zien dat het op analoge wijze verkregen lichaam $\mathbf{Q}_{17}$ zowel een wortel uit -1 als een wortel uit 2 bevat.

5. Concrete p-adische getallen

We kiezen nu een vast priemgetal p, en definiëren het lichaam $\mathbf{Q}_p$ van p-adische getallen heel concreet als bestaande uit elementen gegeven door een oneindige p-adische expansie

$$c_{-m}c_{-m+1}c_{-m+2}\dots c_{-1}, c_0c_1c_2c_3c_4\dots,$$

met m een natuurlijk getal dat per element kan verschillen, en alle cijfers c_k in $\{0,1,2,3,\dots,p-1\}$. We denken aan deze expansie als de *Laurentreeks*

$$\frac{c_{-m}}{p^m}+\frac{c_{-m+1}}{p^{m-1}}+\frac{c_{-m+2}}{p^{m-2}}+\ldots+\frac{c_{-1}}{p}+c_0+c_1\cdot p+c_2\cdot p^2+c_3\cdot p^3+c_4\cdot p^4+\dots,$$

een 'machtreeks in p waarin een *eindig* aantal negatieve machten van p toegestaan zijn', steeds met coëfficiënten $c_k \in \{0,1,2,3,\dots,p-1\}$. Merk op dat dit lijkt op een decimale expansie, waarbij we voor '$p=10$' de decimale verzameling cijfers krijgen, maar in de expansie zelf $p=\frac{1}{10}$ moeten nemen. Een p-adisch getal waar $m=0$ gekozen kan worden, en waarvoor dus alle cijfers c_k met $k<0$ gelijk aan 0 zijn, heet *p-adisch geheel*. Dit zijn de 'gewone' machtreeksen in p, zonder 'cijfers voor de p-adische komma', die ook wel als $c_0c_1c_2c_3c_4\dots$ genoteerd worden.

De p-adische gehele getallen vormen een *deelring* $\mathbf{Z}_p \subset \mathbf{Q}_p$. Het optellen of vermenigvuldigen van elementen in $\mathbf{Z}_p$ gaat net als het van de basisschool bekende vermenigvuldigen van gehele getallen in basis 10, met als voornaamste verschil dat we hier met *oneindige* 'sommen' van p-machten te doen hebben, zodat er oneindig veel cijfers in een som of product uit te rekenen zijn, maar voor ieder cijfer de berekening eenvoudig en eindig

is. Bij de berekening kunnen er cijfers c_k groter dan $p-1$ ontstaan, zijn, en die brengt men net als in het decimale geval terug in de gewenste standaardverzameling $\{0,1,2,3,\ldots,p-1\}$ van cijfers door zo vaak als nodig een cijfer c_k met p te verlagen en ter compensatie c^{k+1} met 1 te verhogen. Op deze manier bepaalt men 'van laag naar hoog' de cijfers van een som of product, en in onze p-adische notatie betekent dat 'van links naar rechts'. (Wie de analogie tussen p en de decimale 10 benadrukken wil kan p-adische expansies ook andersom schrijven, en oneindig door laten lopen naar links.)

Voorbeeld. Voor het 5-adische getal $i \stackrel{5}{=} 21213423032204132\ldots$ met de eerste 17 cijfers als berekend in de vorige paragraaf begint de 5-adische expansie van i^2 als

$$i^2 = 44444444444444444\ldots,$$

en 5-adisch geldt inderdaad $1 + 44444444444444444\ldots \stackrel{5}{=} 0$.

Opgave 11. Bereken i^3 in 17 cijfers nauwkeurig in $\mathbf{Z}_5$.

De 'gewone' gehele getallen liggen als deelring $\mathbf{Z} \subset \mathbf{Z}_p$ in de p-adische getallen. Positieve getallen in $\mathbf{Z}$ schrijft men namelijk eenvoudig in basis p, wat aanleiding geeft tot een p-adisch getal met een *eindige* expansie, en voor een negatief getal $-x \in \mathbf{Z}$ krijgt men $-x \in \mathbf{Z}_p$ door het positieve getal $x \in \mathbf{Z}$ in $\mathbf{Z}_p$ te vermenigvuldigen met $-1 \in \mathbf{Z}_p$, het p-adische getal met cijfers $c_k = p-1$ voor alle $k \geq 0$.

Opgave 12. Laat zien dat voor een p-adisch getal $x \stackrel{p}{=} c_0c_1c_2c_3c_4\ldots \in \mathbf{Z}_p$ met $c_0 \neq 0$ de additieve inverse $-x \stackrel{p}{=} d_0d_1d_2d_3d_4\ldots$ verkregen wordt door $d_0 = 5-c_0$ en $d_k = 4-c_k$ voor $k \geq 1$ te nemen. Hoe volgt hier het algemene geval uit?

Een p-adische *eenheid* is een element $x \stackrel{p}{=} c_0c_1c_2c_3c_4\ldots \in \mathbf{Z}_p$ met $c_0 \neq 0$. Voor dergelijke elementen, die de *eenhedengroep* $\mathbf{Z}_p^* \subset \mathbf{Z}_p$ vormen, kunnen we een multiplicatieve inverse $x^{-1} \stackrel{p}{=} d_0d_1d_2d_3d_4\ldots \in \mathbf{Z}_p$ bepalen door de vergelijking

$$x \cdot x^{-1} \stackrel{p}{=} (c_0c_1c_2c_3c_4\ldots)\cdot(d_0d_1d_2d_3d_4\ldots) \stackrel{p}{=} 1$$

op te lossen. Voor het nulde cijfer vinden we $c_0d_0 = 1 \bmod p$, en deze vergelijking heeft een unieke oplossing $d_0 \in \{0,1,2,3,\ldots,p-1\}$, omdat $c_0 \neq 0$ een multiplicatieve inverse heeft modulo het *priemgetal* p. Het cijfer d_k bepalen we voor ≥ 1 *inductief* uit de eerdere cijfers als oplossing van

$$c_0d_k = -(c_1d_{k-1} + c_2d_{k-2} + \cdots + c_{k-1}d_1 + c_kd_0) \bmod p.$$

Ook hier is er een unieke oplossing $d_k \in \{0, 1, 2, 3, \ldots, p-1\}$.

Opgave 13. Bepaal de 5-adische expansie van $\frac{1}{7} \in \mathbf{Z}_5$, en laat zien dat deze periodiek is.

Opgave 14. Laat zien dat zowel de decimale expansie van $\frac{1}{7} \in \mathbf{R}$ als de p-adische expansie van $\frac{1}{7} \in \mathbf{Z}_p$ voor $p = 3$ en $p = 5$ periodiek zijn met een periode van lengte 6. *Welke andere periodelengtes komen er voor als we p variëren? **Komen deze periodelengtes voor voor oneindig veel priemgetallen $p \neq 7$?

In $\mathbf{Z}_p$ is vermenigvuldiging met p een eenvoudige operatie, waarbij alle cijfers 1 plek naar rechts worden opgeschoven:

$$p \cdot (c_0 c_1 c_2 c_3 c_4 \ldots) \stackrel{p}{=} 0 c_0 c_1 c_2 c_3 c_4 \ldots .$$

Hieruit zien we dat ieder element $x \neq 0$ in $\mathbf{Z}_p$ uniek te schrijven is als een product $x = p^m \cdot u$ voor een eenheid $u \in \mathbf{Z}_p^*$ en een natuurlijk getal m, dat de *valuatie* van x heet. Een p-adisch getal $x \in \mathbf{Q}_p$ buiten $\mathbf{Z}_p$ kunnen we schrijven als

$$x \stackrel{p}{=} c_{-m} c_{-m+1} c_{-m+2} \ldots c_{-1}, c_0 c_1 c_2 c_3 c_4 \ldots \in \mathbf{Q}_p$$

met $c_{-m} \neq 0$ en $m \geq 1$, en hiervoor hebben we $x = p^{-m} \cdot u$ voor de eenheid $u \stackrel{p}{=} c_{-m} c_{-m+1} c_{-m+2} \ldots c_{-1} c_0 c_1 c_2 c_3 c_4 \ldots \in \mathbf{Z}_p^*$. In dit geval is de valuatie $-m$ van x een *negatief* geheel getal.

Opgave 15. Laat zien dat op $\mathbf{Q}_p^* = \mathbf{Q}_p \setminus \{0\}$ de valuatieafbeelding $v_p : \mathbf{Q}_p^* \to \mathbf{Z}$ gedefinieerd door $v(p^m \cdot u) = m$ voldoet aan $v_p(xy) = v_p(x) + v_p(y)$.

De valuatieafbeelding v_p, die op $\mathbf{Q}^*$ het 'aantal factoren p' in een rationaal getal aangeeft, ligt ten grondslag aan de p-adische afstand op $\mathbf{Q}$, die we zometeen zullen definiëren.

Opgave 16. Laat zien dat een reëel getal $x \neq 0$ uniek geschreven kan worden als $x = 10^m \cdot u$, met $\frac{1}{10} < |u| \leq 1$ en $m \in \mathbf{Z}$ de entier van $-^{10}\log |x|$.

Uit de schrijfwijze van de elementen $x \in \mathbf{Q}_p^* = \mathbf{Q}_p \setminus \{0\}$ als $x = p^m \cdot u$, met $m \in \mathbf{Z}$ de valuatie van x en $u \in \mathbf{Z}_p^*$ een p-adische eenheid, zien we dat alle $x \in Que_p^*$ binnen $\mathbf{Q}_p$ een multiplicatieve inverse $x^{-1} = p^{-m} \cdot u^{-1} \in \mathbf{Q}_p$ hebben. Dit maakt $\mathbf{Q}_p$ tot een *lichaam*. Het is het *quotiëntenlichaam* van de ring $\mathbf{Z}_p$ van p-adisch gehele getallen, net zoals $\mathbf{Q}$ het quotientenlichaam is van de ring $\mathbf{Z}$ van 'gewone' gehele getallen. Uit de inclusie $\mathbf{Z} \subset \mathbf{Z}_p$ krijgen we in het bijzonder een inclusie $\mathbf{Q} \subset \mathbf{Q}_p$.

Opgave 17. Laat zien: een rationaal getal $x = \frac{a}{b} \in \mathbf{Q}$ met $\gcd(a, b) = 1$ ligt in $\mathbf{Z}_p$ dan en slechts dan als p geen deler is van b.

6. De p-adische completering van $\mathbf{Q}$

Het lichaam $\mathbf{R}$ van reële getallen kan men, even concreet als we dat voor $\mathbf{Q}_p$ gedaan hebben, definiëren in termen van elementen gegeven door een 'decimale expansie'. Zo'n concrete beschrijving lijkt echter van allerlei keuzes af te hangen – te beginnen met de representatie van gehele getallen in het tientallig stelsel. Een wat abstractere beschrijving begint vaak met het lichaam $\mathbf{Q}$ van rationale getallen, en verkrijgt de reële getallen als *limieten* van rijtjes rationale getallen onder het 'natuurlijke' afstandsbegrip tussen rationale getallen gegeven door de absolute waarde. Dit is een formalisering van het intuïtieve begrip van het dichtstoppen van de 'gaatjes' tussen de rationale getallen. Een soortgelijke beschrijving kan ook gegeven worden van het lichaam $\mathbf{Q}_p$, als completering van $\mathbf{Q}$ onder het p-adische afstandsbegrip.

De p-adische absolute waarde van een rationaal getal wordt verkregen in termen van van de al gedefinieerde valuatie $v_p : \mathbf{Q}^* \to \mathbf{Z}$. Ieder rationaal getal $x \neq 0$ is namelijk te schrijven als $x = p^m \cdot u$, met $m = v_p(x) \in \mathbf{Z}$ de p-adische valuatie van x en $u = \frac{a}{b}$ een rationaal getal waarvan teller noch noemer deelbaar is door p. Men definieert nu de p-adische absolute waarde op $\mathbf{Q}$ door

$$|x|_p = \begin{cases} p^{-m} & \text{als } x \neq 0 \text{ en } v_p(x) = m; \\ 0 & \text{als } x = 0. \end{cases}$$

Deze absolute waarde is net als de 'gewone' absolute waarde multiplicatief op $\mathbf{Q}$:

$$|xy|_p = |x|_p |y|_p \qquad \text{voor } x, y \in \mathbf{Q}.$$

De p-adische absolute waarde van een geheel getal $x \in \mathbf{Z}$ is echter nooit groter dan 1, en x is p-adisch erg klein als hij 0 is modulo een *hoge* macht van p. Voor de bijbehorende *p-adische afstand* op $\mathbf{Q}$, gegeven door

$$d_p(x, y) = |x - y|_p,$$

betekent dit, dat gehele getallen dicht bij elkaar liggen als ze congruent zijn modulo een hoge macht van p.

Men kan de elementen van $\mathbf{Q}_p$ nu definiëren als de p-adische limieten van rijtjes rationale getallen, net als reële getallen 'gewone' limieten zijn van rijtjes rationale getallen. Zulke limieten hebben automatisch een absolute waarde, die gelijk is aan de limiet van de absolute waarden van de benaderingen. Op de precieze details van dit proces, de *completering* met betrekking tot een afstandsfunctie, gaan we hier niet verder in.

Het verkregen resultaat $\mathbf{Q}_p$ hangt (net als in het geval van $\mathbf{R}$) er niet af van welke precieze benaderingen door rationale getallen men gebruikt.

Voor $\mathbf{R}$ zijn benaderingen gegeven door decimale en binaire expansies populair, voor $\mathbf{Q}_p$ hebben we zojuist de bekendste concrete beschrijving gegeven. Het is echter zeer wel mogelijk andere cijferverzamelingen dan $\{0, 1, 2, \ldots, p-1\}$ te gebruiken: iedere verzameling van p cijfers die in verschillende restklassen modulo p liggen is geschikt. Voor oneven p is bijvoorbeeld $\{0, \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$ een andere mogelijkheid.

Opgave 18. Laat zien dat voor $p = 5$ de verzameling bestaande uit 0, $\pm i$, ± 1 een geschikte cijferzameling is die bovendien *multiplicatief gesloten* is.

In plaats van machtreeksen in p zelf kan men ook machtreeksen gebruiken in $p \cdot u$ voor een p-adische eenheid u.

Opgave 19. Laat zien dat als we de elementen van $\mathbf{Q}_p$ representeren als $\sum_k a_k(-p)^k$ met cijfers $a_k \in \{0, 1, 2, \cdots, p-1\}$, *alle* $x \in \mathbf{Z}$ een eindige expansie hebben.

De p-adische afstand op $\mathbf{Q}$ is een *ander* afstandsbegrip dan het afstandsbegrip $d(x, y) = |x - y|$ behorende bij de 'gewone' absolute waarde. Een fundamenteel verschil is dat de bekende *driehoeksongelijkheid*

$$|x + y| \leq |x| + |y|$$

voor rationale getallen x en y onder de p-adische afstand verscherpt kan worden tot de *ultrametrische ongelijkheid*

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}.$$

Deze ongelijkheid volgt uit de ongelijkheid $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$ voor de p-adische valuatie voor $x, y \in \mathbf{Q}^*$ met $x + y \neq 0$.

Opgave 20. Geef een compleet bewijs voor de ultrametrische ongelijkheid, geldig voor $x, y \in \mathbf{Q}_p$, en laat zien dat voor $|x|_p \neq |y|_p$ *gelijkheid* optreedt.

De ultrametrische ongelijkheid laat zien dat alle open en gesloten 'bollen'

$$B(r) = \{x \in \mathbf{Q}_p : |x_p| < r\} \qquad \text{en} \qquad D(r) = \{x \in \mathbf{Q}_p : |x_p| \leq r\}$$

van straal $r \in \mathbf{R}_{>0}$ rond de oorsprong in $\mathbf{Q}_p$ gesloten zijn onder optelling. Voor $r = 1$ zien we dat de *ring* $D(r) = \mathbf{Z}_p$ van p-adisch gehele getallen de 'gesloten eenheidsschijf' is in $\mathbf{Q}_p$.

Het *archimedische principe*, dat zegt dat een reëel getal $x > 0$, mits voldoende vaak bij zichzelf opgeteld, willekeurig groot gemaakt kan worden, geldt kennelijk niet voor de *niet-archimedische* p-adische afstand. De 'meetkunde' van het niet-archimedische lichaam $\mathbf{Q}_p$ verschilt daardoor van de vertrouwde meetkunde van $\mathbf{R}$ en het platte vlak.

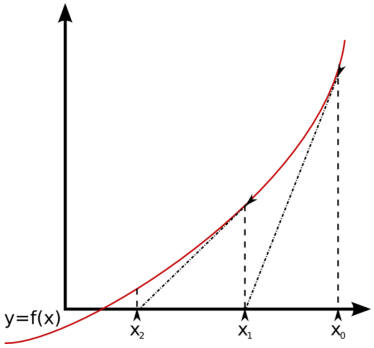
Om te beginnen heeft de bekende *totale ordening* van $\mathbf{R}$, die zegt dat voor twee verschillende reële getallen $x, y \in \mathbf{R}$ altijd $x < y$ of $y < x$ geldt, geen analogon voor $\mathbf{Q}_p$. In het bijzonder zijn er geen 'positive' of 'negatieve' p-adische getallen, en kan men $\mathbf{Q}_p$ beter niet met een lijn identificeren. Ook een identificatie met 'punten in een vlak', die geen ordening hebben, is moeilijk.

Opgave 21. Laat zien dat ieder punt x in de 'open schijf' $B(y, r) = \{x \in \mathbf{Q}_p : |x_p| < r\}$ van straal $r > 0$ rond $y \in \mathbf{Q}_p$ een middelpunt is: $B(x, r) = B(y, r)$.

Opgave 22. Laat zien dat iedere driehoek xyz in $\mathbf{Q}_p$ gelijkbenig is: van de drie afstanden $d_p(x, y)$, $d_p(x, z)$ en $d_p(y, z)$ zijn er tenminste twee gelijk.

7. Hensel's lemma en idempotenten in $\mathbf{Z}_{10}$

De compleetheid van $\mathbf{Q}_p$ heeft tot gevolg dat sommige methodes die voor een compleet lichaam als $\mathbf{R}$ ontwikkeld werden, met kleine aanpassingen ook voor $\mathbf{Q}_p$ gebruikt kunnen worden. Dit is bijvoorbeeld het geval met de *Newton-Raphson-methode* voor het benaderen van nulpunten van functies.



Hierbij verbetert men een 'benaderend' nulpunt x_0 van een differentieerbare functie $f : \mathbf{R} \to \mathbf{R}$ door de raaklijn in het punt $(x_0, f(x_0))$ te doorsnijden met de x-as, en de x-coördinaat van het snijpunt $(x_1, 0)$ als 'verbeterde' benadering. Als formule:

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}.$$

Of x_1 daadwerkelijk een verbeterde benadering is, hangt van de omstandigheden af – in ongelukkige gevallen is de raaklijn horizontaal, of ligt x_1 juist verder van het gezochte nulpunt af – maar in den regel krijgt men 'in de

buurt' van het gezochte nulpunt een snelle convergentie van benaderende nulpunten $x_0, x_1, x_2, \ldots$ door de Newton-formule te itereren.

Voor het polynoom $f(x) = x_2 - 2$ hebben we

$$x_{k+1} = x_k - \frac{x_k^2 - 2}{2x_k} = \frac{x_k}{2} + \frac{1}{x_k},$$

en de reële beginwaarde $x_0 = 1$ geeft achtereenvolgens, op 10 decimalen nauwkeurig

$$1, \quad 1.5, \quad 1.4166666667 \quad 1.4142156863 \quad 1.4142135624 \quad 1.4142135624.$$

In 7 stappen krijgt men zo de eerder gegeven reële benadering van $\sqrt{2}$ tot op meer dan 50 decimalen nauwkeurig.

Passen we nu *dezelfde* formule toe op de wortel $x_0 = 3$ van $2 \in \mathbf{Q}_7$, waarvoor $x_0^2 - 2 \equiv 0 \bmod 7$ geldt, dan krijgen we 7-adisch de rij

$$\begin{aligned}
x_1 &\stackrel{7}{=} 31111111111111111111\ldots \\
x_2 &\stackrel{7}{=} 31260332531126033253\ldots \\
x_3 &\stackrel{7}{=} 31261212352532610460\ldots \\
x_4 &\stackrel{7}{=} 31261212466211020333\ldots \\
x_5 &\stackrel{7}{=} 31261212466211021146\ldots
\end{aligned}$$

die snel convergeert naar een wortel $\sqrt{2} \in \mathbf{Q}_7$. Als in het reële geval *verdubbelt* de precisie van een voldoend goede benadering in elke stap.

Opgave 23. Benader $\sqrt{-1} \in \mathbf{Q}_5$ met behulp van bovenstaande methode nauwkeurig tot op zestien 5-adische cijfers.

Hensel's lemma zegt dat voor een polynoom $f \in \mathbf{Z}_p[x]$ en een *enkelvoudig* nulpunt x_0 modulo p, ofwel een element $x_0 \in \mathbf{Z}_p$ met $f(x_0) = 0 \bmod p$ en $f'(x_0) \neq 0 \bmod p$, de uitkomst van Newton-iteratie *altijd* naar een nulpunt in $\mathbf{Z}_p$ convergeert. Deze stelling is een stuk *eenvoudiger* dan in het reële geval, waar algemene convergentie-resultaten veel lastiger te bewijzen zijn.

Opgave 24. Bewijs dit lemma.
[Hint: gebruik de 'Taylorbenadering' $f(x+h) = f(x) + hf'(x) +$ 'hogere orde termen...]

Als recreatieve toepassing kan men Newtoninteratie ook toepassen in de ring $\mathbf{Z}_{10}$, die men krijgt door in de constructie van $\mathbf{Z}_p$ doodleuk $p = 10$ te nemen, en te vergeten dat 10 geen priemgetal is. Hierin hebben we de waarde $x_0 = 6$, die modulo 10 een nulpunt is van het kwadratische polynoom $f(x) = x^2 - x$. Onze iteratieformule geeft nu

$$x_{k+1} = x_k - \frac{x_k^2 - x_k}{2x_k - 1},$$

en men kan zich met enige zorg afvragen of zo'n 'deling' modulo niet-priemgetallen wel altijd mogelijk is. Opgave aan de lezer: voer de iteratie uit, en leg uit wat er nu gebeurt!

8. Locaal-globaal-principes

Als een Diophantische vergelijking met rationale coëfficiënten rationale oplossingen heeft, dan heeft hij in het bijzonder oplossingen in $\mathbf{R}$ en in $\mathbf{Q}_p$ voor alle p. Omdat het bestaan van punten over $\mathbf{R}$ of over $\mathbf{Q}_p$, juist door de 'compleetheid' van die lichamen, meestal zeer makkelijk na te gaan is, geeft dit een veel gebruikte methode om te laten zien dat bepaalde vergelijkingen geen rationale oplossingen hebben.

Zoals we eerder in iets andere terminologie lieten zien, heeft de hyperbool H met vergelijking $3x^2 + 2 = y^2$ wel punten met coördinaten in $\mathbf{R}$, maar niet in $\mathbf{Q}_2$ of $\mathbf{Q}_3$. In het bijzonder heeft H dus geen rationale punten. Omgekeerd kan men zich afvragen of een vergelijking die wel oplosbaar is over alle completeringen van $\mathbf{Q}$, ook een oplossing over $\mathbf{Q}$ moet hebben. Deze vraagstelling, die met name door Hensel's leerling Hasse in grote algemeenheid werd gesteld, heeft een centrale plaats in de moderne arithmetische meetkunde gekregen.

Helmut Hasse (1898–1971)

Men kan laten zien ('stelling van Ostrowski') dat $\mathbf{R}$ en de lichamen $\mathbf{Q}_p$ de enige completeringen van $\mathbf{Q}$ ten opzichte van 'absolute waardes' zijn, en men noemt een vergelijking over $\mathbf{Q}$ die over al die completeringen oplossingen toestaat, een *locaal overal oplosbare vergelijking*. Er zijn klassen van vergelijkingen, zoals kegelsneden, waarvoor een locaal overal oplosbare

vergelijking ook *globaal oplosbaar* is, hetgeen betekent dat de vergelijking een rationale oplossing heeft. Men zegt in zo'n geval dat het *Hasse-principe* voor de vergelijking geldt.

In zijn algemeenheid is het niet waar dat een locaal overal oplosbare vergelijking ook altijd globaal oplosbaar is. Al voor vergelijkingen van graad 3, het eenvoudigste geval na dat van kegelsneden en kwadrieken, gaat het mis. Er zijn vlakke krommen van graad 3, nauw gelieerd aan de sinds Wiles' bewijs van Fermat zeer populaire elliptische krommen, waarvoor het Hasse-principe *niet* geldt. In dit cubische geval laat zich de obstructie tegen het Hasse-principe concretiseren in Tate-Shafarevich-groep van elliptische krommen. Het Hasse-principe geldt voor een elliptische kromme dan en slechts dan als deze Tate-Shafarevich-groep uit 1 element bestaat, oftewel 'triviaal is' Op dit moment kunnen we nog niet eens bewijzen dat Tate-Shafarevich-groepen van elliptische krommen over $\mathbf{Q}$ altijd *eindig* zijn – er is nog het nodige te doen in de aritmetische meetkunde!

Literatuur.

1. Fernando Q. Gouvêa, *p-adic numbers, an introduction (Second Edition)*, Springer Universitext, 1997.
2. Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions (Second Edition)*, Springer Graduate Text in Mathematics, 1984.
3. P. Stevenhagen, *Algebra 1, 2, 3*, Mathematisch Instituut, Leiden, 2014; een online versie is beschikbaar op `websites.math.leidenuniv.nl/algebra`.
   [Dit zijn de drie syllabi die gebruikt worden in de wiskundebachelor in Leiden.]

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
E-mail: `psh@math.leidenuniv.nl`

4 Intuïtie, inzicht, bewijs

Aad Goddijn
Freudenthal Instituut, Universiteit Utrecht

4. 1 Verklaring ter inleiding

Als wiskundig amateur houd ik meer van inzicht dan van bewijs. Als zoeker naar inzicht begin ik liever bij mijn intuïties dan bij axioma's. Ik zeg het maar van te voren: tot U spreekt een ketter die, althans vandaag, de deductieve drie-eenheid *Gegeven, Te bewijzen, Bewijs* niet als hoogste goed ziet. Ik wil echter geen fundamentalist zijn; ik zal met respect spreken over grote andersdenkenden en hun mooie verhalen trouw doorgeven.
De programmacommissie van deze cursus vroeg mij te laten zien, dat het voor het begrijpen van een meetkundig bewijs nogal wat uit kan maken of de taal van de algebra of die van lijnen en cirkels wordt gekozen; misschien is de vraag geïnspireerd door de op handen zijnde herinvoering van Analytische Meetkunde in het examenprogramma VWO-B en een deel van mijn meningen hangt daar ook mee samen. Er is uiteraard het triviale soms-zus-soms-zo antwoord, maar dat geef ik niet; ik wijs er liever op dat de twee methoden bij dezelfde opgave soms verschillende problemen lijken op te lossen. Ik ga dit tamelijk informeel verder toelichten, maar harde bewijzen - als voorbeeld, en binnen de wiskunde - zullen er ook zijn. Voorbeelden kies ik vooral omdat ik plezier in ze heb en op grond van beperkingen van tijd en ruimte; zo doe je dat als amateur.

4. 2 Hoe vind je het midden van een lijnstuk?

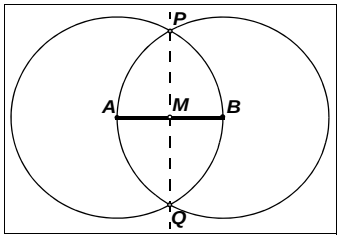
Afgelopen lente maakte ik vliegers met een groepje kinderen; van die ouderwetse latjes en papiervliegers. De actie vond plaats bij de jaarlijkse familiedag, waar broers en zusters van mijn generatie met hun kinderen en kleinkinderen bij elkaar komen. Dit jaar was er muziek voor de allerkleinsten en vliegers maken voor de oudere kinderen (7 tot 12), alles gezellig samen met ouders, grootouders en andere familieleden.
Een klassieke pijl-en-boog vlieger heeft een gebogen dwarslat en een staande lat. Het buigen van de dwarslat dient de stabiliteit van de vlieger; heeft een rondgebogen vlieger even één zijde iets meer naar voren in de windrichting, dan staat die zijde meer dwars op de wind dan de andere zijde en de stand van de vlieger wordt daardoor automatisch gecorrigeerd.
Het is uiteraard belangrijk dat het midden van de dwarslat goed bepaald wordt. De standaardmethode gebruikt een meetlint of rolmaat. Zo: leg het meetlint langs de lat met de 0 bij het begin van de lat, lees de lengte af, deel het gevonden getal

door twee, zoek de uitkomst op het meetlint op en zet daar een streepje op de lat. Deze methode staat bekend als de methode van de Analytische Meetkunde. Daarbij wordt een getallenlijn (of meerdere getallenlijnen) aan de probleemsituatie toegevoegd en wordt rekenen (en soms algebra) gebruikt om onbekende lengtes te vinden die de eigenlijk oplossing van het probleem vormen.
Zevenjarige Anna wist nog niet hoe je zo'n midden kunt vinden.
Ik vroeg haar een streepje te zetten waar het zo ongeveer zou moeten zitten. Dat doet ze. Daar:

Mooi, dan kijken we of het klopt. Leg de lat even links tegen de tafelrand en zet ook het streepje op de tafel:

Draai de lat nu eens om.

Ach, het klopt niet helemaal. Je kunt nu wel een béter streepje zetten: tussen de twee streepje in. Is het midden nu gevonden? Ja, voor vliegers is dit goed genoeg. Dit is de methode van het Iteratief Verbeteren. Wiskundigen begrijpen snel dat de verbeteringstap onbeperkt herhaald kan worden. Ze kunnen zelfs bewijzen, dat als bij elke stap grof wordt misgegokt, bijvoorbeeld als wordt ingedeeld niet in de buurt van de verhouding 1 : 1 maar bijvoorbeeld steeds in 1 : 100, dat zelfs dán op den duur met elke gewenste nauwkeurigheid het midden bepaald wordt.
Op de vliegermiddag ontbrak de methode die in ruim drieëntwintighonderd jaar meetkunde-onderwijs favoriet was, die met passer en liniaal. Dit is de methode van de Synthetische Meetkunde. Vanuit twee gegeven punten *A* en *B* wordt met behulp van cirkels en lijnen volgens strenge regels een nieuw punt, *M*, geconstrueerd. Een bewijs dat alleen teruggrijpt op eerder bewezen zaken of op vooraf overeengekomen axioma's, moet daarna uitwijzen dat het geconstrueerde punt inderdaad het midden van *AB* is.



4. 3 Intuïtie ≠ inzicht ≠ bewijs

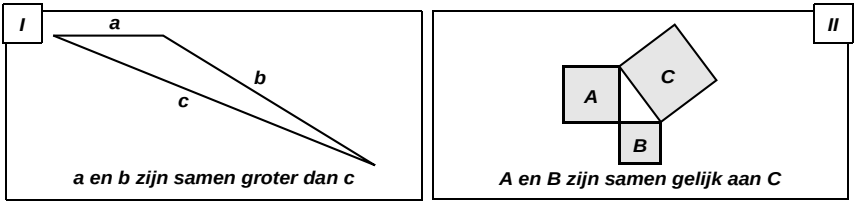
Hoe triviaal het vliegervoorbeeld ook lijkt, de verschillen tussen de drie methodes zijn dat niet, en niet alleen in wiskundig opzicht.
De analytische methode (met meetlint) levert snel een middelpunt op, de praktische waarde van de methode is groot. Inzicht lijkt minder van belang; het is een

methode voor doeners, doeners die zich niet door twijfel aan de methode laten belemmeren. Deze methode geeft ons overigens ook de lengte van de lat en de lengte van de helft van de lat als bijproducten. Die werden niet gevraagd; vanuit een oogpunt van elegantie en efficiency is dat een lelijke smet op het werk. De weinig filosofische doener zal dit bestrijden: de helft van 41 op de getallenlijn *is* toch het midden van 0 en 41. Jawel, maar dat is op de getallenlijn. Dit heeft te maken met een visie over meetkunde, waarin de getallenlijn niet een gereedschap is zoals een hamer voor timmerman, maar een echt onderdeel van de objecten, zoals een ronde houten lat dat is in een klerenkast. Ik kom hier later nog kort op terug, onder het kopje 'schoolboekmeetkunde'.

De synthetische methode (met passer en liniaal) slaat hier nog wilder om zich heen; de cirkels waarmee begonnen wordt lijken niets met het probleem te maken te hebben. Alleen genieën weten dat zo'n contra-intuïtieve ingreep de juiste is.

Is deze methode praktisch? Mijn vlieger makende familie vindt waarschijnlijk van niet. Inzichtelijk? Niet zonder meer, tenzij je het bewijs dat nog geleverd moet worden bij voorbaat al inzicht noemt. Bij de synthetische meetkunde (zoals we die kennen uit *De Elementen* van Euclides [6]) gaat het er vooral om dat we meetkundige objecten construeren vanuit basiselementen als punt, lijn en cirkel. Daarbij ligt sterk de nadruk op de logische structuur die uitgangspunten als 'door elk tweetal punten gaat één lijn' uiteindelijk verbindt met uitspraken als 'de drie hoogtelijnen van een driehoek gaan door één punt'. De meetkunde van Euclides is dan ook hét voorbeeld van de deductieve methode in de wetenschap. Nieuwe zekerheid leunt daar alleen op al voorhanden zekerheden. Wat een wiskundig bewijs precies is, kan hier strak omschreven worden.

'Inzicht' is voor mij toch wat anders 'bewijs'. Daarin speelt persoonlijke beleving mee; het is een psychologisch begrip. Mag ik even een criminele metafoor gebruiken? Soms kan een DNA-match een bewijs rond maken, dat persoon *A* persoon *B* iets lelijks heeft aangedaan. Maar dit geeft geen inzichtelijk antwoord op de vraag waaróm *A* dat gedaan heeft. Ook binnen de meetkunde zijn 'inzicht' en 'bewijs' verschillend. Neem de twee figuren hieronder. Wij (wiskundig geschoolden) weten zeker dat de beweringen onder deze twee figuren (binnen het kader van die 2300 jaar oude meetkunde) juist zijn.



Toch denk ik dat de bewering in geval I heel dicht bij onze intuïtieve inzichten aansluit en die van geval II niet.

Voor bewering II hebben we nauwelijks draagvlak in onze eigen dagelijkse ervaring. Bewering II is wel vele malen en op vele manieren bewezen. Bewering I is echter helemaal niet zo eenvoudig binnen het kader van de traditionele meetkunde te bewijzen, hoe 'evident' de bewering ook is. Euclides zelf gaat erbij in zijn beroemde Elementen zelfs de fout in.
Al we een intuïtief oordeel over iets vellen, dan is het eigenlijk zo dat we oordelen met behulp van uitgebreide kennis over voorgaande, verwante en analoge ervaringen, maar dat we ons dat niet bewust zijn op het moment van oordelen zelf. Zo zie ik het althans op dit moment en maak daarmee intuïties los van influisteringen door muzen of andere geheimzinnige wezens. Daarmee houd ik ook de deur open voor de ware wiskundige die wél intuïties ervaart rond de stelling van Pythagoras en over nog veel meer. Die heeft zoveel verwante en analoge wiskundige ervaringen, dat voor haar/hem die stelling één is geworden met zijn denken en voelen. Een van mijn bewonderde docenten van vroeger, professor Nicolaas Kuiper (1920-1994), vertelde dat hij zo vertrouwd was met complexe getallen en i, dat die voor hem helemaal niet abstract meer waren. Maar hij kon goed begrijpen dat ze dat voor ons nog wél waren. Vooral voor die laatste toevoeging ben ik hem nog steeds dankbaar.

De iteratieve methode (met herhaald gebruik van het timmermansoog) blijft van de drie het dichtst bij het doel van het zoeken van het midden. Het is mijn favoriet, althans bij vliegers. De methode is intuïtief sterk. Maar de degelijke wiskundige fundering van het herhalingsproces en het effect daarvan kan alleen rusten op preciseren van begrippen als benaderen, tot in het onbeperkte (het oneindige?) doorgaan, limieten, enzovoort. Anna's vlieger vloog prima zonder die fundering. In de rest van dit verhaal zullen we de kenmerken van deze drie methodes in complexere situaties nog herhaaldelijk ontmoeten, al geef ik wegens beperkte tijd de derde minder ruimte dan de andere twee.

4. 4 Korte geschiedenis

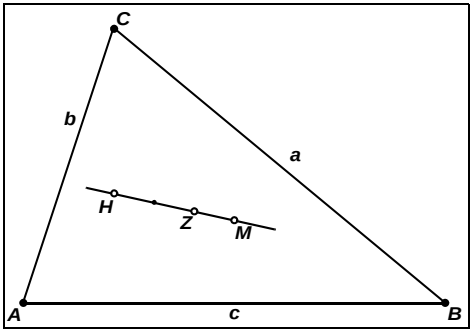
Als besluit van deze inleiding geef ik iets uitgebreider aan wat met Analytische Meetkunde bedoeld wordt aan de hand van een klein stukje geschiedenis.
Descartes [3] beweert in zin één van zijn essay *La Géométrie* dat elk meetkundig probleem gereduceerd kan worden tot het vinden van lengtes van lijnstukken. In de analytische methode zoals hij die daarna aan ons demonstreert, wordt een meetkundig probleem vertaald in algebra; daarbij krijgen gegeven lijnstukken gegeven lengtes *a, b, c, ...* en krijgen onbekende lijnstukken onbekende lengtes *x, y, z, ...* . In principe worden uiteindelijk *x, y, z, ...* in *a, b, c, ...* uitgedrukt, of worden er verbanden tussen *x, y, z, ...* gevonden. Als we van *x* en *y* als lengtes overstappen naar posities op twee (of meer) gegeven onderling loodrechte (getallen)lijnen, hebben we onze traditionele Analytische Meetkunde van vlak of ruim-

te te pakken. De analytische methode is echter niet gebonden aan het zogenaamd Cartesisch assenstelsel, ook algebraïsch werken met poolcoördinaten, vectoren, complexe getallen hoort er voor mij allemaal bij.
Voor vandaag is deze oppervlakkige beschrijving voldoende, maar de ontstaansgeschiedenis van dit huwelijk van meetkunde en algebra is boeiend en instructief. Zie bijvoorbeeld het geschiedenishoofdstuk van *Wat a is kun je niet weten* (Drijvers [5]) voor een compacte beschrijving aan de hand van Descartes' eigen tekst. Descartes zelf zag zijn methode als een speciale vorm voor het vinden van een in principe synthetische constructie, die noodzakelijk na het vinden van de algebraïsche oplossing als nog uitgevoerd diende te worden. Later werd de algebraïsche stap, in het bijzonder het vinden van de onbekende '*x*' alleen al als 'de oplossing' van het gegeven meetkundige probleem gezien. Voor een zeer uitvoerige en diepgaande analyse bespreking van Descartes' ideeën , zie Bos [2]: *Redefining Gemetrical Exactness: Descartes' transformation of the early modern concept of construction*.

4. 5 Virtuoos rekenwerk aan de lijn van Euler

We gaan nu als eerste voorbeeld een meetkundestelling bekijken die middels de analytische methode is ontdekt en bewezen; we zullen zien dat de analytische methode hier met grote virtuositeit werd beoefend. Onze held is Leonard Euler (1707 - 1783) zelf.
De stelling waar het om gaat is welbekend:

> *In elke driehoek liggen het hoogtepunt H, het zwaartepunt Z en het middelpunt M van de omgeschreven cirkel op een rechte lijn en bovendien verdeelt Z het lijnstuk HM in de verhouding 2 : 1 in.*



Zie de figuur hiernaast. De lijn heet uiteraard de rechte van Euler. Euler vond en bewees de stelling als eerste in 1767.
Nu volgt een samenvatting van het oorspronkelijke analytische bewijs van Euler. Ik leun hierbij sterk op *Euler, The Master of Us All* van William Dunham [4], die de oorspronkelijk Latijnse tekst vertaalde en rijk becommentarieerde.
Eulers werkplan is snel samengevat. Hij legt punt *A* op de oorsprong van een coördinatenstelsel en *B* op de positieve *x*-as ervan. Hij berekent dan de coördinaten van *H*, *Z* en *M*. Preciezer: hij drukt die uit in de lengtes *a*, *b*, *c*, van de zijden.
Daarna worden de lengtes van *HZ*, *ZM* en *HM* berekend, ook weer uitgedrukt in *a*, *b*, *c*. (Die lengtes noteren we verder als $\overline{HZ}$, $\overline{ZM}$ en $\overline{HM}$). Euler toont vandaar

uit aan dat $\overline{HZ} = 2\,\overline{ZM}$ en $HM = 3\,\overline{ZM}$. Omdat $\overline{HZ} + \overline{ZM} = \overline{HM}$, ligt Z volgens de driehoeksongelijkheid óp het lijnstuk HM én deelt dat lijnstuk in 2 : 1 in.
Het plan in deze samenvatting bevat geen enkele uit de lucht vallende stap en het is principieel in de keuze van de lengtes van de zijden a, b, c als de letters waarin de zaken uitgedrukt gaan worden.
In de berekeningen zelf zit het harde werk én is de virtuositeit van Euler te zien. Van dit rekenwerk laat ik hier slechts een klein deel zien; Eulers gehele bewijs beslaat in Dunham [4] negen pagina's.

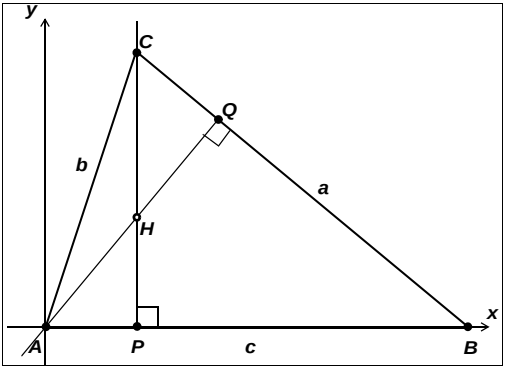
Euler gebruikt als hulpgrootheid de oppervlakte K van de driehoek en de beroemde formule van Heron die K in de zijden a, b, c van de driehoek uitdrukt. Bij de Heron-formule wordt meestal de halve omtrek van de driehoek $(a + b + c)/2$ met de letter s aangegeven. Herons formule is dan:

$$K = \sqrt{s(s-a)(s-b)(s-c)}$$

(Voor enkele fraaie bewijzen, zie het schitterende *Wat te bewijzen was* van Martin Kindt [12]. Euler heeft zelf in 1748 ook een kort en krachtig synthetisch bewijs van die formule gegeven, zie weer Dunham [4].)
K^2 kan natuurlijk zonder wortel en zonder s in a, b en c worden uitgedrukt, iets wat later gebruikt gaat worden. Een kleine vooroefening voor wat komen gaat:

$$\begin{aligned} 16K^2 &= 16s(s-a)(s-b)(s-c) \\ &= (b+c+a)(b+c-a)(a+c-b)(a+b-c) \\ &= ((b+c)^2 - a^2)(a^2 - (b-c)^2) \\ &= (b^2 + 2bc + c^2 - a^2)(a^2 - b^2 + 2bc - c^2) \\ &= 2a^2b^2 + 2b^2c^2 + 2a^2c^2 - a^4 - b^4 - c^4 \end{aligned}$$

Nu gaan de coördinaten van H bepaald worden. Natuurlijk moeten we aan de hand van de liggingen in de figuur nu formules opstellen. Descartes beweert dat voor het opstellen van de vergelijkingen tussen de bekenden en onbekenden alleen gelijkvormigheidseigenschappen en de stelling van Pythagoras nodig zijn. Hij overtreedt een enkele maal zijn eigen grenzen, maar Euler blijft binnen die beperking.



We gebruiken de hoogtelijnen uit C en uit A.
$\overline{AP}$ is de x-coördinaat van H. CP is de gemeenschappelijke rechthoekszijde van

twee rechthoekige driehoeken. Tweemaal *Pythagoras* levert een gelijkheid op

$$b^2 - \overline{AP}^2 \;=\; a^2 - (c - \overline{AP})^2$$

zodat

$$\overline{AP} \;=\; \frac{b^2 + c^2 - a^2}{2c}$$

Voor het bepalen van HP gaan we de *gelijkvormigheid* van ΔAPH en ΔAQB gebruiken. We hebben nu $\overline{QA}$ en $\overline{BQ}$ nodig. Zie hier:

$$\overline{QA} \;=\; \frac{2K}{a} \qquad \overline{BQ} \;=\; \frac{c^2 + a^2 - b^2}{2a}$$

$\overline{BQ}$ is net zo als $\overline{AP}$ gevonden; vertalen van a, b, c naar b, c, a kan ook.
Met behulp van de gelijkvormigheid volgt nu:

$$\begin{aligned}\overline{HP} \;&=\; (\overline{BQ} \cdot \overline{AP}) / \overline{QA} \;=\; \left(\frac{a^2 + c^2 - b^2}{2a}\right)\left(\frac{b^2 + c^2 - a^2}{2c}\right) / \left(\frac{2K}{a}\right) \\ &=\; \frac{2a^2b^2 - a^4 - b^4 + c^4}{8cK} = \frac{16K^2 - 2a^2c^2 - 2b^2c^2 + 2c^4}{8cK} \\ &=\; \frac{2K}{c} + \frac{c(c^2 - a^2 - b^2)}{4K}\end{aligned}$$

Daarmee is ook de y-coördinaat van H in a, b en c uitgedrukt.

De laatste stappen lopen via de uitdrukking voor $16K^2$ van zo-even. Euler werkt hier met het oog op latere samenhang met de formules voor de punten Z en M naar een equivalente vorm om.
De coördinaten van Z en M worden via andere - maar eveneens eenvoudige - meetkundestappen gevonden. De tamelijk omvangrijke afleidingen laat ik verder achterwege. De resultaten bij Euler zijn:

Coördinaten van *H:* $\left(\frac{b^2 + c^2 - a^2}{2c}, \frac{2K}{c} + \frac{c(c^2 - a^2 - b^2)}{4K}\right)$

Coördinaten van *Z:* $\left(\frac{3c^2 + b^2 - a^2}{6c}, \frac{2K}{3c}\right)$

Coördinaten van *M:* $\left(\frac{c}{2}, \frac{c(a^2 + b^2 - c^2)}{8K}\right)$

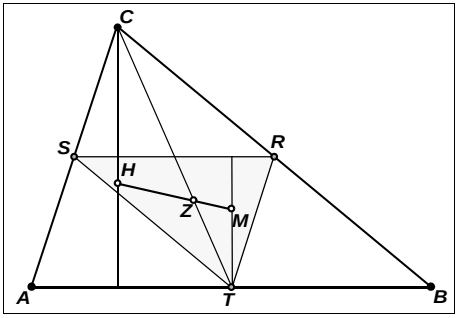
Van hier uit is het nog een lange algebraïsche weg naar $\overline{ZM}^2$, $\overline{HZ}^2$ en $\overline{HM}^2$ en het bepalen van hun verhoudingen. Men controlere bijvoorbeeld maar eens dat:

$$\overline{ZM}^2 \;=\; \frac{(b^2 - a^2)^2}{36c^2} - \frac{2a^2 + b^2 + c^2}{12} + \frac{a^2b^2c^2}{16K^2}$$

Euler bereikt uiteindelijk de verhouding 1 : 4 : 9 waaruit de gevraagde verhouding,de gelijkheid $\overline{HZ} + \overline{ZM} = \overline{HM}$, en de collineariteit volgen. Bewijs voltooid.

De kracht van de analytisch methode lijkt overduidelijk: de meetkundige moeilijkheden zijn zeer gering, *en de algebraïsche moeilijkheden lijken dat ook*. Het is veel, maar wie ijverig, geduldig en nauwkeurig is, zou het moeten kunnen? Nee! Bij Euler is het heel planmatig georganiseerd wat betreft algebraïsche vorm van de tussenresultaten. Zonder dat superinzicht was het niet gelukt.

4. 6 De rechte van Euler, dat is toch triviaal?



Zwaartelijn *CT* wordt, dat is bekend, door het zwaartepunt *Z* in de verhouding 2 : 1 ingedeeld.
Dat betekent: draaien we *CZ* over 180° om *Z* en vermenigvuldigen we de lengte met een factor 1/2, dan belandt *C* op *T*.
Deze zelfde draaivermenigvuldiging rond *Z* voert de hele driehoek *ABC* over in driehoek *RTS*. De hoogtelijn uit *C* wordt dan overgevoerd in de middelloodlijn van *AB*. Soortgelijks geldt voor de andere hoogtelijnen. Daaruit volgt dat *H* overgaat in *M*.
Dus *H, Z* en *M* liggen op één lijn en $\overline{ZM} = 1/2\ \overline{HZ}$, ofwel $\overline{HZ} = 2\ \overline{ZM}$.

4. 7 Methoden vergelijken (1)

De kracht van het zojuist gegeven synthetische bewijs ligt in het gebruik van een actie, die een werking op het *geheel* van de figuur inhoudt. Het is een beweging die visueel is, je ziet het gebeuren. Onze intuïtie neemt in de draai het geheel mee, de driehoek mét zijn hoogtelijnen. Zo hebben we hebben overzicht, en kijk op de relatie tussen details en het geheel. Begrip? Inzicht? Ik denk het wel.
Dit in grote tegenstelling tot de eerdere analytische aanpak, waar we algebraïsch steeds in het lage kruipelhout ronddwaalden. Zo'n gelijkheid als ,

$$16K^2 = 2a^2b^2 + 2b^2c^2 + 2a^2c^2 - a^4 - b^4 - c^4$$

die in de *algebra* van het bewijs functioneert, kan niet in de *meetkunde* van de figuur betekenisvol worden aangewezen.
Toch is er ook een ander groot verschil tussen de methoden, waarbij de analytische aanpak juist wel wint.
Stel je voor dat we de stelling nog niet kenden en dat de hele berekening van Euler niet uitgelopen was op $\overline{HZ} = 2\ \overline{ZM}$ maar op $\overline{HZ} = \mathbf{3}\ \overline{ZM}$. Dan had de analy-

tische aanpak ons die factor 3 aangereikt op het moment dat de formule voor $\overline{HZ}^2$ door Euler door die voor $\overline{ZM}^2$ algebraïsch werd gedeeld en als uitkomst '9' verscheen. Verhoudingsfactor 3 werd dan op dat moment eigenlijkt *ontdekt*. Bij de synthetische aanpak gebruiken we de factor 2, het bewijs is geheel daarop gebaseerd. De analytische aanpak is hier dus ook een ontdekkingsroute, de synthetische is dat eigenlijk niet, de toont alleen al aanwezige vermoedens aan.
De beroemde fysicus Richard Feynman vatte zijn visie op het verschil tussen de analytische en de synthetische methode samen in een nabeschouwing bij zijn synthetische afleiding van de ellipsvorm van de planeetbanen uit de zwaartekrachtwet van Newton. Daarin gaat het ook over ontdekken en bewijzen:

> *It is not easy to use the geometrical method to discover things. It is very difficult, but the elegance of the demonstrations after the discoveries are made is really very great.*
>
> *The power of the analytic method is that it is much easier to discover things than to prove things. But not in any degree of elegance. It's a lot of dirty paper, with x's and y's and crossed out cancellations and so on.* [7]

Feynman zegt ook dat het hem veel moeite en vindingrijkheid kostte elementaire meetkundige bewijzen bij zijn probleem van de ellipsbaan te vinden. Maar, eenmaal gevonden, konden ze in elegante vorm gepresenteerd worden.
Euler liet ons zijn *dirty paper* en *crossed out cancellations* niet zien, als hij ze al had. Maar we weten ook niet hoe het korte synthetische bewijs tot stand is gekomen! Prachtige invallen lijken zulke bewijzen, snel als bliksemschichten, maar dat er soms lang op ze gewacht moet worden en of ze het product van lang polijsten zijn, wordt zelden verteld.

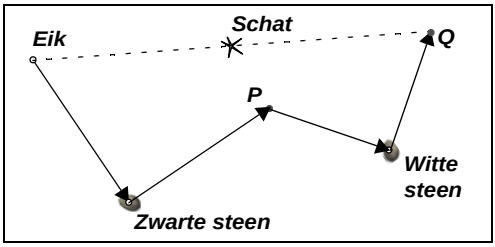
Het lijkt er in eerste instantie wel op dat het synthetische bewijs hier met een bijzondere methode werkt, die als het ware uniek voor het probleem is, terwijl het analytische bewijs duidelijk een heel algemene methode gebruikt.
Dat is hier maar zeer ten dele zo, al is het wel een van de standargumenten tégen de synthetische methode: te weinig algemene techniek, teveel afhankelijk van de persoonlijke vondst. We zullen zien of dat in dit geval zo is!

4. 8 Schatgraven op Teleurstellingseiland: complex of triviaal?

Sommige problemen hebben zowel een mooie analytische oplossing als een mooie synthetische oplossing. Kom mee naar *Teleurstellingseiland* omdat te beleven. Daar ligt een schat. Je hebt een oude aanwijzing:

> *De schat ligt verborgen op Teleurstellingseiland. Coördinaten: 50°36.25 Zuid, 165°58.38 Oost. Je vindt een stomp van een oude eik, een zwarte en een witte steen. Ga op de stomp staan, loop naar de zwarte steen, draai 90° naar links en loop nog eens precies dezelfde afstand. Loop nu naar de*

witte steen, draai 90° naar links en loop nogmaals dezelfde afstand. Graaf midden tussen jou en de stomp.



Natuurlijk maken we een kladje vooraf.
Op Teleurstellingseiland aangekomen vinden we snel de zwarte en de witte steen. Maar geen stomp van een eik!
We proberen het natuurlijk toch: gewoon érgens beginnen en doen alsof de eik daar heeft gestaan. Wat een geluk: we vinden direct de schat!

Opgave 1. Laat zien dat de aangewezen plaats van de schat niet van die van de eik afhangt. Probeer het eerst zelf, er zijn vele methoden mogelijk die anders zijn dan de nu volgende twee.

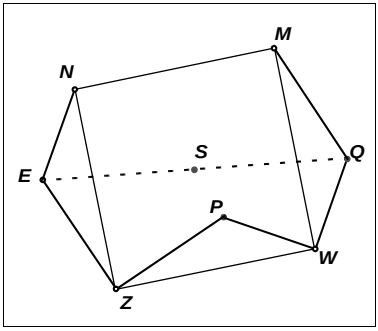
4.8.1 Analytische oplossing in het complexe vlak

Omdat er in uet schtagraafprobleem draaien over 90° zonder verkorten of verlengen voorkomen , kiezen we voor werken met het complex vlak. Immers: vermenigvuldigen met **i** is daar tegenkloks draaien over 90°, en vermenigvuldigen met **-i** is draaien over 90° met de klok mee.
Zien we ons kladje als het complexe vlak, dan bevat de oude aanwijzing een paar regels algebra:

$$E - Z = i(P - Z) \qquad Q - W = -i(P - W)$$

$$Schat = \frac{E + Q}{2} = \frac{Z + i(P - Z) + W - i(P - W)}{2} = \frac{Z + W + i(W - Z)}{2}$$

De laatste uitdrukking is alleen afhankelijk van de stenen en kan ook nog geïnterpreteerd worden als het midden van het vierkant op *ZW*.



4.8.2 Synthetische (?) oplossing

Vull de figuur aan met vierkant *ZWMN* en zeshoek *ZWQMNE*. Die is puntsymmetrisch om *S*. Het punt *S* is ook midden van het vierkant *ZWMN* en dus alleen bepaald door *Z* en *M*. Het is weer eens triviaal.

4. 9 Methoden vergelijken (2)

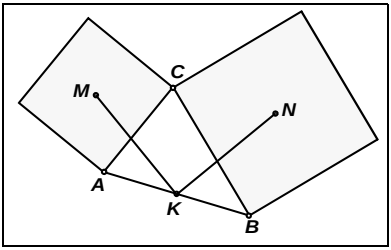
Helemaal niet triviaal! De korte oplossing bij *Teleurstellingseiland* is een praatje achteraf. Als je al wéét dat *S* het midden van het vierkant op *ZW* is, kun je dat

vierkant gaan tekenen en dan lacht het korte ‘bewijs’ je met zijn drie gelijke driehoeken al toe.
Het is vaak mogelijk bij meetkundeproblemen korte bewijzen te construeren, als er al andere - bottere - bewijzen voorhanden zijn die de structuur onder het probleem hebben opengelegd. Dat is hier bij het vierkant echt wel het geval.
Maar het synthetische bewijs bij de Eulerlijn hierboven staat los van het algebraïsche bewijs van Euler zelf. De reden waarom het analytische bewijs bij Teleurstellingseiland wél een pure meetkundige constructie suggereert, is dat we hier in de analytische aanpak niet zomaar met coördinaten werken, maar met een systeem dat de loodrechte draai al in zich heeft. Anders gezegd: de keuze van het algebraïsch hulpmiddel is bij Teleurstellingseiland vergaand op het probleem afgesteld, terwijl die keuze bij de Eulerlijn dat niet is.
Bij de Eulerlijn is ook een analytisch bewijs mogelijk met behulp van vectoren, dat kort en heel elegant is. Zie weer *Wat te bewijzen was* van Martin Kindt [12].
Leg de driehoek zó in een tweedimensionale vectorruimte, dat de oorsprong O het hoogtepunt van de driehoek is. Laten de hoekpunten aangewezen zijn door vectoren m_1, m_2, m_3. Het zwaartepunt Z is dan $(m_1 + m_2 + m_3)/3$. Het snijpunt M van de middelloodlijnen moet liggen op de lijn die door $(m_1 + m_2)/2$ gaat en evenwijdig is aan de hoogtelijn op zijde m_1m_2; m_3 heeft precies die richting, omdat we driehoek zo hebben neergelegd. Dus $M = (m_1 + m_2)/2 + \lambda m_3$ voor een of ander waarde van λ. Net zo vinden we via zijde m_1m_3 dat $M = (m_1 + m_3)/2 + \mu m_2$ voor een of andere waarde van μ. Omdat m_2 en m_3 verschillende richtingen hebben, is er geen geen keus voor λ en μ; het moet zijn $\lambda = \mu = 1/2$.
Dus $M = (m_1 + m_2 + m_3)/2$. We zien $M = 3/2\ Z$. Bewijs klaar!
Evenwijdigheid, werken met verhoudingen: daarom zijn vectoren hier hét uitgelezen middel, passend bij het gegeven vraagstuk. Het kiezen van de oorsprong als hoogtepunt, dat is natuurlijk wel een vondst.

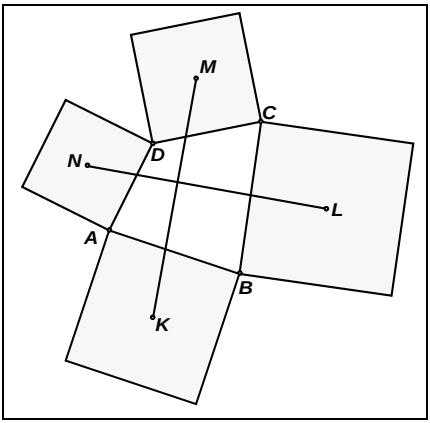
4. 10 Opgaven: gebruik i, vul tekening aan

Als er rechte hoeken of vierkanten een rol spelen, zoals bij Teleurstellingseiland, dan loopt een gang naar het complexe vlak vaak op een feestje uit.

Opgave 2. Twee vierkanten op een driehoek.
Bouw vierkanten op AC en BC van driehoek ABC. Laten M en N de middens van die vierkanten zijn en laat K het midden van AB zijn.
Toon aan: MK en NK staan loodrecht op elkaar en $\overline{MK} = \overline{NK}$.

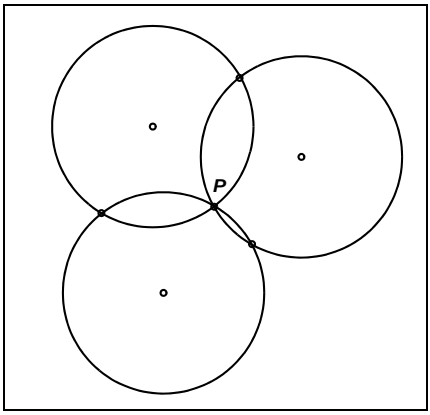


Opgave 3. Vier vierkanten op een vierhoek.
Ga uit van een willekeurige vierhoek *ABCD* en bouw vierkanten op de vier zijden, alle vier naar buiten toe. Laten *K*, *L*, *M*, en *N* de middens zijn van de vierkanten. Toon aan dat *KM* en *LN* even lang zijn en loodrecht op elkaar staan.



Opgave 3 kan heel goed met gebruik van het rechtse draaigetal **i** geheel zelfstandig worden opgelost. Het is handig om een formule te maken die bij gegeven *P* en *Q* een volgend punt van het vierkant op *PQ* geeft. Een andere mogelijkheid is eerst opgave 2 gebruiken op twee helften van de vierhoek, namelijk op driehoeken *ACD* en *CAB* en dan de resultaten op een of ander manier koppelen.

Opgave 4. Drie gelijke cirkels a*anvullen*.
Gegeven drie cirkels met gelijke straal die door één punt *P* gaan. Er zijn nog drie snijpunten, telkens van twee cirkels.
Teken de cirkel door die drie punten.



Toon aan dat die cirkel dezelfde straalheeft als de eerste drie cirkels.
Aanvullingstip: Teken de zeshoek van de gegeven middelpunten en snijpunten en maak die figuur met *P* en een nog te vinden punt af tot een kubus.

In David Wells [15] meldt dit als ontdekking van Roger Johnson uit 1916. Roger Johnson is auteur van een klassieke tekst: *Advanced Euclidean Geometry.* [9].

4. 11 Examenopgave verduistert mooie oplossing

In het vernieuwde VWO-B wiskunde programma komt het domein *Meetkunde met coördinaten* voor. In 2014 zijn er pilotexamens geweest.
Op een bijeenkomst met docenten werden opgaven daaruit aan de tand gevoeld; ik was er bij. De opgave waar het om gaat neem ik in zijn geheel hier op.

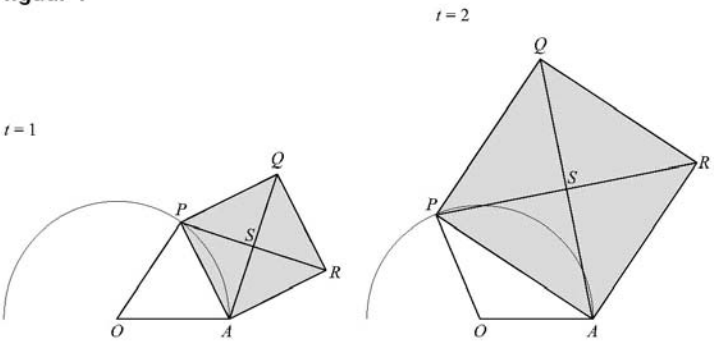
Vierkant op een driehoek

Gegeven zijn de punten $O(0, 0)$ en $A(2, 0)$.
Punt P beweegt over de halve cirkel met middelpunt O en straal 2 volgens de bewegingsvergelijkingen

$$\begin{cases} x(t) = 2\cos t \\ y(t) = 2\sin t \end{cases} \quad \text{met } 0 < t < \pi$$

Tegen de zijde AP van driehoek OAP ligt een vierkant $ARQP$. Dit vierkant ligt buiten driehoek OAP. Punt S is het snijpunt van de diagonalen van vierkant $ARQP$. In figuur 1 is de situatie op de tijdstippen $t = 1$ en $t = 2$ weergegeven.

figuur 1



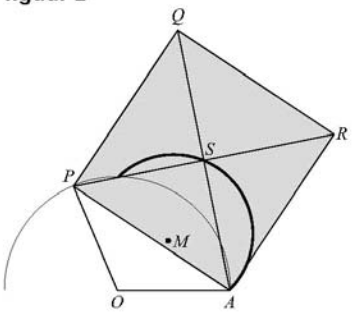
Er geldt: $\overrightarrow{OS} = \begin{pmatrix} 1 + \cos t + \sin t \\ 1 - \cos t + \sin t \end{pmatrix}$

4p **11** Bewijs dit.

In figuur 2 is een deel getekend van de baan waarover S beweegt tijdens de beweging van punt P. Figuur 2 doet vermoeden dat de baan van S een cirkel is met middelpunt $M(1, 1)$.

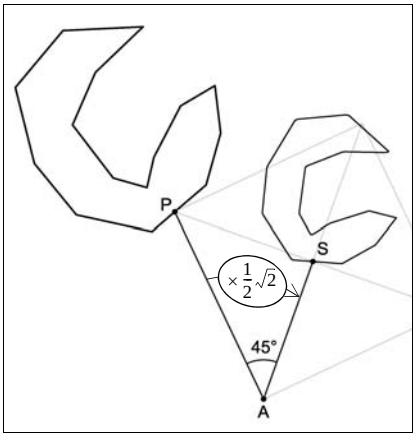
4p **12** Bewijs dat de afstand van S tot het punt $M(1, 1)$ constant is.

figuur 2



Op de docentenbijeenkomst tuinde ik er in en liet me volkomen aan de dwingende hand nemen door de ontwerpers van de opgave. Met enige moeite worstelde ik me door de twee vragen waarmee we op het analytische pad werden gestuurd. Tot ik weer zonder analytische blinddoek naar de figuur keek ....

In deze figuur is te zien hoe bij punt P het punt S wordt gevonden. Voor elk punt P wordt AP om draaipunt A over $45°$ naar rechts gedraaid, en ingekort met een factor $\frac{1}{2}\sqrt{2}$.



De baan van S is een verkleinde om A gedraaide kopie van de baan van P. Het doet er daarbij niet toe wat de figuur is waar P over loopt. Daar is S.
De ligging van de halve cirkel die S in de oorspronkelijke vraag doorloopt en de ligging van het middelpunt zijn nu ook duidelijk verklaard uit de beweging $P \rightarrow S$ en niet uit eigenschappen van de functies cosinus en sinus.
(Uiteraard ligt M midden tussen begin en eind van de halve cirkel die S doorloopt en niet zo slordig als in de gegeven figuur 2).
Dat de opdracht uitloopt op een op zich mooi resultaat werd de leerlingen niet van meet af aan getoond als bewijsdoel van de opgave. In plaats daarvan wordt een rekenkeurslijf opgedrongen waarin de dingen zitten die getoetst moeten worden. Ik begrijp best dat gekozen is voor een examenopgave waarin de vaardigheden van de analytische methode worden getoetst. Maar het lijkt me geen reclame voor de analytische methode dit te doen met een opgave die beter met een intuïtief veel sterkere methode kan worden opgelost.

De aanwezigheid in je hoofd van sterke beelden als de draaivermenigvuldiging geeft toegang tot een redeneerwereld die veel dichter bij je intuïtie ligt dan de hier opgedrongen technieken uit de analytische wereld. Ik ben er hard voor dat in het meetkunde-onderwijs zulke sterke visuele methoden aan bod komen die het niveau van punt-voor-punt werken overstijgen en waarbij het werken met een figuur als geheel productief is.
Dat gebruik van zo'n algemeen meetkundig inzicht misschien moeilijker te toetsen is dan algebraïsche vaardigheden mag geen rem zijn op dit pleidooi. Meetkundig inhoudelijke keuzes moet prioriteit houden op exameneisen. Toetsbaarheid is geen criterium voor zinvolheid van een wiskundige methode. Dit in 2015 even terzijde; de officiële nieuwe examens zijn in 2017.

Ter afsluiting drie opgaven als vervolg hierop.

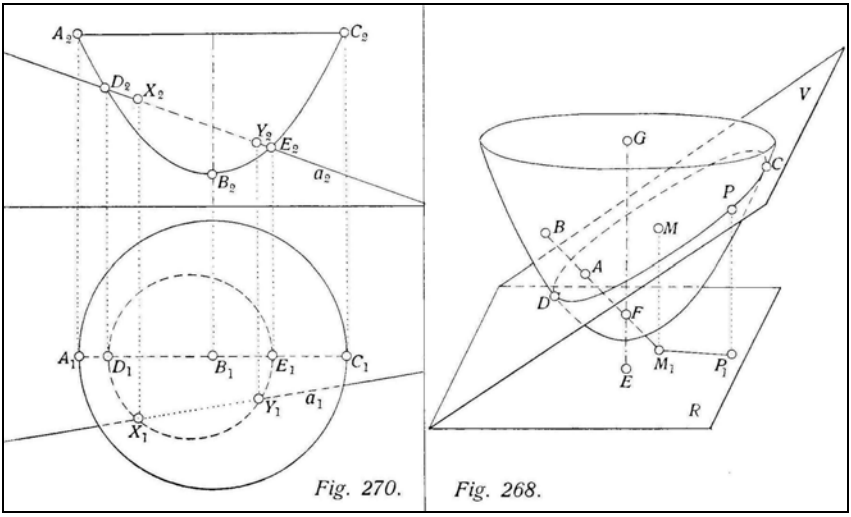
Opgave 5. (Makkelijk!)
Laat zien dat *Q* en *R* in de opgave ook halve cirkels beschrijven.

Opgave 6. (Gebruik een stukje vers verouderde meetkunde)
In figuur 2 in de oorspronkelijke opgave lijkt het zo dat de lijn *PR* door het begin van de halve cirkel gaat waar *S* op ligt, d.w.z. door punt (0, 2). Toon aan dat dit zo is.

Opgave 7. (Verbetering definitie van het vierkant in de opgave)
Uiteraard werkt de oplossing met de draaivermenigvuldiging ook als in plaats van de halve cirkel waar *P* op loopt, een hele cirkel wordt gebruikt.
Maar de manier waarop het vierkant in de opgave in het pilotexamen is vastgelegd geeft dan een minder fraai resultaat: twee halve cirkels die samen géén hele cirkel vormen.
Vraag: Hoe zou de definitie van het vierkant *ARPQ* in de kop van de opgave moeten worden aangepast, dat het wél goed gaat?
Tip: kijk hoe in Geogebra met de optie 'regelmatige veelhoek' aan beide zijden van een lijnstuk *AB* naar keuze vierkanten kunnen worden gezet. Gebruik het idee 'omloopsrichting' hier. Merk op dat de vastlegging van het vierkant in de opgave van het te transformeren object afhangt, wat gewoon erg onhandig is.

4. 12 Een paraboloïde snijden met een vlak

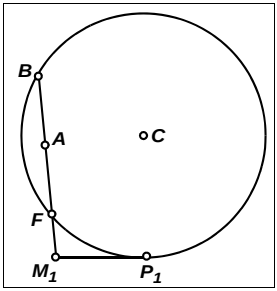
De indruk is intussen wel gewekt dat als het om elegantie gaat, de synthetische methode het meestal genadeloos wint van de analytische. In deze paragraaf een voorbeeld waarbij dat niet zomaar het geval is. De fraaie tekening (volgende bladzijde) komt uit de atlas - het afzonderlijk figurenboek- bij *Leerboek der Beschrijvende Meetkunde* van W. A. Piets [13] uit 1908.
Links in de figuur het koppel van voor- en bovenaanzicht, zoals gebruikelijk bij Beschrijvende Meetkunde. De figuur rechts is nu onze leidraad; een parallelprojectie die de situatie suggestief in beeld brengt: een doorsnijding van een omwentelingsparaboloïde met een vlak *V*.
V snijdt de paraboloïde in een kromme. In het bovenaanzicht (links, onderste figuur) is te zien dat de projectie van die kromme op het grondvlak een cirkel is. Dat is het resultaat waar het om gaat en het is goed even te bedenken dat dit iets bijzonders is. Ook als het vlak *V* een steile hoek met het grond vlak maakt, en de doorsnijding dus heel langwerpig kan zijn, is die projectie een cirkel. Dit gaan we op twee manieren bewijzen, eerst synthetisch op de wijze die Piets zelf beschrijft, daarna analytisch in 3D.
De paraboloïde is hier gedefinieerd als de verzameling punten die de zelfde af-



stand hebben tot het richtvlak *R* en tot het brandpunt *F*. In de figuur is *P* een punt van de snijkromme. Punt *B* is het spiegelbeeld van *F* in het snijvlak *V; A* is het midden van *FB* en ligt dus in *V*. Punt M_1, dat zo dadelijk gebruikt gaat worden, is het snijpunt van lijn *BF* met het grondvlak *R*. P_1 is de loodrechte projectie van *P* op grondvlak *R*.

De spelers zijn geïntroduceerd, nu het spel!

Uit de constructie van *B* en de definitie van de paraboloïde volgt direct dat $\overline{BP} = \overline{FP} = \overline{P_1P}$. Vanwege de loodrechte stand van PP_1 op vlak *R*, raakt vlak *R* aan die bol in punt P_1. Piets en zijn doelgroep van vroeg twintigste eeuwse techniekstudenten in Delft, wisten dan meteen dat $\overline{M_1P_1}^2 = \overline{M_1F} \cdot \overline{M_1B}$ en P_1 dus op een cirkel met middelpunt M_1 ligt, omdat het rechterlid van deze gelijkheid constant is. Einde van het korte bewijs.



Misschien is er behoefte bij de moderne lezer om $\overline{M_1P_1}^2 = \overline{M_1F} \cdot \overline{M_1B}$ apart veilig te stellen door het vlak waarin *B, F,* M_1 en P_1 liggen, uit te lichten. De bol snijdt dat vlak volgens een cirkel waar M_1P_1 aan raakt. De rest zal wel lukken via de gelijkvormigheid van ΔFP_1M_1 en ΔP_1BM_1 of door *B, A, F* en P_1 met middelpunt *C* te verbinden en Pythagoras te gebruiken en wat te rekenen.

Op zich is dit een mooi bewijs, maar -zoals al eerder gezegd bij synthetische bewijzen - de niet ingewijde begrijpt absoluut waarom

die eerste magische zet (spiegelen van F in V) gedaan wordt. Laten wij in 2015 wel bedenken dat dit voorbeeld staat op bladzijde 353 van een uitgebreid leerboek. Voor de lezer van toen was het zo helder als het volgende analytische bewijs het waarschijnlijk voor ons is. Hier komt het.
Kies een 3-dimensionaal coördinatenstelsel met x- en y-as in het grondvlak R en kies als z-as de as van het omwentelingslichaam, dat de paraboloïde is. De paraboloïde is (bij juiste schaling) dan gegeven door de vergelijking $z = x^2 + y^2$ en het vlak V door $z= ax + by +c$. De x- en y-waarden van de punten in de doorsnijding voldoen aan $x^2 + y^2 = ax + by +c;$ dat is de vergelijking van de projectie van de doorsnijding. Ja, dat is een cirkel!

4. 13 Oude schoolboekmeetkunde, Hilberts Grundlagen

De zegepalm voor elegantie leek zo-even naar de algebra te gaan, maar een nuancering is toch wel nodig. De gegeven analytische aanpak gaat uit al meteen uit van de vergelijking van de paraboloïde; dat is natuurlijk wel een stap die al genomen moet zijn. De synthetische methode begon echt met de definitie van de paraboloëde. Anders gezegd: de analytische methode kreeg (nam) hier een voorsprong, door van een iets ander probleem uit te gaan. Toch een klein beetje vals spel. Herinneren we ons ter vergelijking dat Euler met zijn virtuose analytische bewijs juist uitging van de driehoek als gegeven door de drie lengtes van de zijden en niet van een driehoek met handige coördinaten. Dat was eerlijk en moedig!
Terwijl de analytische methode oorspronkelijk een middel is om een meetkundeprobleem aan te pakken, worden in de meeste oude schoolboeken over Analytische Meetkunde de meetkundige vraagstukken al onmiddellijk in coördinatenverpakking aangeleverd. Voor oefenvraagstukken is dat ook wel voor de hand liggend.
Ellips, parabool en hyperbool werden meestal wel geïntroduceerd via de bekende afstandskenmerken, op meetkundige wijze dus. Maar daarna worden direct de standaardvergelijkingenen afgeleid in het theoriedeel van de hoofdstukken, dat eigenlijk de uitlegtaken voor de docent vastlegde. De zware nadruk op de standaardvergelijkingen gaf waarschijnlijk wel de indruk dat van kegelsneden de assen altijd evenwijdig aan de assen van het coördinatenstelsel liepen, met uitzondering van de orthogonale hyperbool, waar de asymptoten dat deden. De standaardvergelijkingen zijn precies de tweedegraadsvergelijkingen in x en y die geen kruisterm xy hebben. De theorie bevatte soms wel de techniek om bij een algemene tweedegraadsvergelijking met kruisterm zodanig op ander coërdinaten over te gaan, dat de kruisterm verdween.
Na de theorie volgden vraagstukken voor de leerling, Daar speelde deze achtergrond geen rol. De leerling werd ook zelden de keus van methode analytisch of synthetisch overgelaten. Hier volgen drie vraagstukken uit de altijd veel geprezen

Beknopte Analytische Meetkunde van Dr. D. J. E. Schrek [14], alle drie in aanpak anders; een zuiver meetkundige opgave, een rekenoefening, een meetkundige vraag met ingebakken analytisch gereedschap. 17 en 19 zijn interessant. Maar wie zit er te wachten op de hoek en de oppervlakte van vraag 18?

17. Door het brandpunt van een parabool trekt men een willekeurige koorde. Bepaal de meetkundige plaats van het snijpunt der raaklijnen, die in de uiteinden der koorde aan de parabool kunnen worden getrokken.
18. In elk der snijpunten van de cirkel $x^2 + y^2 = 18$ en de parabool $y^2 = 3x$ trekt men aan beide krommen de raaklijn.
    a. Bereken de scherpe hoek, die deze raaklijnen in elk snijpunt met elkaar maken.
    b. Bereken de oppervlakte en de omtrek van de vierhoek, die door de vier raaklijnen wordt ingesloten.
19. Van $\triangle$ ABC zijn de hoekpunten B$(+ a, 0)$ en C$(- a, 0)$ vast. De top A beweegt zich over de lijn $y = b$. Bepaal de meetkundige plaats van het hoogtepunt van die driehoek.

In een professioneel bedoeld boek als de zeer uitvoerige *Analytische Meetkunde* van Barrau [1] wordt in deze zaken veel consequenter, maar ook een stuk abstracter opgetreden. Daar wordt niet uitgegaan van een al bestaande meetkunde waar de coördinatenmethode overheen wordt gelegd, maar wordt een punt van meet af aan *gedefinieerd* als een greep van twee of drie getallen en worden lijnen als lineaire algebraïsche relaties gedefinieerd. De theoretische achtergronden hiervan, zoals die door Hilbert in zijn G*rundlagen der Geometrie* (1899) [8] zijn beschreven, gaan diep. Ruw geformuleerd gebeurt er dit: Hilbert geeft allereerst een veel sterker axiomastelsel dan het lekkende systeem van de Elementen van Euclides en laat zien dat vanuit die aldus axiomatisch gedefinieerde meetkunde een getallenlichaam kan worden geconstrueerd, met een constructie die op het perspectivisch tekenen van tegelvloeren lijkt. De meetkunde die op de wijze van Barrau bij dat getallenlichaam hoort is dezelfde meetkunde als die we oorspronkelijk hadden.

4. 14 Het mechanisme van Richard Roberts uit Manchester

Het volgende probleem zullen we zien, dat bij een ingewikkeld meetkundig object, soms toch met enige handigheid een vergelijking kan worden gevonden voor de figuur waar het om gaat. Maar wat te doen als de ontstane vergelijking niet zo mededeelzaam is, of - anders gezegd- onze krachten te buiten gaat?
Ik ontleen het voorbeeld aan een prachtige monografie van A. B. Kempe uit 1877 met een geweldige titel: *How to Draw a Straight Line: A Lecture on Linkages* [11]. Het gaat daarin om de vraag hoe met een stangenmechanisme een punt in rechtlijnige beweging gebracht kan worden. Werkelijk rechtlijnig, of in zeer goede benadering. De vraag was in de eeuw van de stoommachine en het massaal ge-

bruikte industriële weefgetouw van groot belang. James Watt zelf heeft er in 1774 al een mooie bijdrage aan geleverd, maar nu onderzoeken we het mechanisme van Richard Roberts (1789-1864), een van de belangrijkste Britse ingenieurs uit de 19e eeuw.
De illustratie komt uit de lecture van Kempe en ademt de geur van stoomlocomotieven, oude scheepswerven en gietijzeren pilaren van Victoriaanse stations.
Kempe:

> *The radial bars are of equal length, the distance between the fixed pivots is twice that of the pivots on the traversing piece, and the tracer is situated on the traversing piece, at a distance from the pivots on it equal to the lengths of the radial bars. The tracer in consequence coincides with the straight line joining the fixed pivots at those pivots and half-way between them. It does not, however, coincide at any other points, but deviates very slightly between the fixed pivots. The path described by the tracer when it passes the pivots altogether deviates from the straight line.*

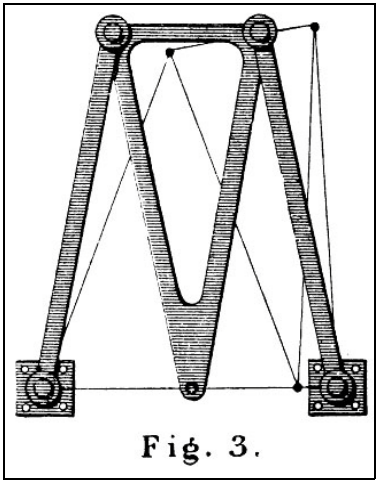
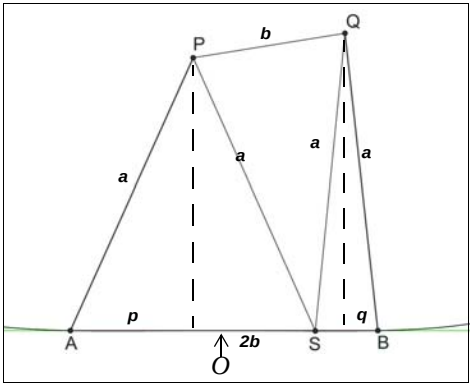


Fig. 3.

De getrokken lijnen laten een andere stand van het mechanisme zien. De grote vraag is of het onderpunt van de hangende driehoek bij het bewegen van het mechaniek langs de grondlijn blijft gaan, want daar is het voor ontworpen. Kempe zegt van niet maar geeft hier geen argumentatie.
In Geogebra kan het mechanisme gemakkelijk worden getekend én bewogen. *A* en *B* zijn hier de vaste punten, de vaste gelijke lengtes zijn aangegeven met *a* en *b*. De baan van *S* is getekend. Inderdaad, afwijkingen tussen *A* en *B* zijn niet te zien en daarbuiten wel.



Mijn intuïtie roept mij nu luid toe dat het heel vreemd is als in de oplossingsverzameling van een algebraïsche vergelijking (want dat is die baan uiteindelijk) een stukje rechte lijn zit dat vloeiend overloopt in een stukje gebogen lijn. Ik vertrouw mijn

intuïtie hier wel, maar dat geeft niemand zekerheid.
Aan Geogebra kunnen we de coördinaten van *S* vragen, en dan krijgen we het heldere antwoord NEE op de vraag of *S* op *AB* ligt. Omdat het antwoord ontkennend is, weten we, (als we de numerieke krachten van Geogebra vertrouwen) dat het ook echt *nee* is. Maar zo eerloos willen we niet ten ondergaan.

Er is een verrassend eenvoudig synthetisch bewijs dat *S* in de niet-triviale standen (het midden, op *A* of *B*) inderdaad *niet* op *AB* ligt. Sieb Kemme vond het; het is een bewijs uit het ongerijmde. Stel je voor dat *S* wél op *AB* ligt. *APS* en *SQB* zijn dan twee gelijkbenige driehoeken met de basissen gewoon aansluitend op grondlijn *AB*. Dan liggen die twee loodlijnen uit *P* en *Q* dus precies afstand *b* uit elkaar. Kijk nu eens naar boven, naar *PQ*. Als die driehoeken *APS* en *SQB* niet congruent zijn, liggen *P* en *Q* niet op gelijke afstanden van de grond lijn en $PQ = b$ is dan niet te rijmen met de afstand *b* tussen de loodlijnen. Een mooie vondst, dit bewijs! Hopelijk komen we analytisch toch nog wat verder, want het synthetische bewijs geeft toch ook maar beperkt resultaat. Het laat bijvoorbeeld niet zien of *S* boven of onder *AB* loopt en geeft ook nog geen inzicht waarom het pad van *S* tussen *A* en *B* zo weinig van de rechte lijn afwijkt.
We zullen daarom een poging doen een vergelijking op te stellen voor $S(x,y)$, al is het maar om te proberen hoe dat uitpakt.
We nemen *AB* als *x*-as en het midden van *AB* als oorsprong. We verwachten -intuïtief, maar zeer terecht- dat de baan van *S* symmetrisch rond de middelloodlijn van *AB* zal zijn. Dat betekent ook dat we alles wat we over *PS* bedenken, via symmetrie kunnen vertalen in iets over *QS*. Dat spaart werk.
In de figuur zijn de loodlijnen uit *P* en *Q* getrokken en de afstanden van hun voetpunten tot *A* en *B* met *p* en *q* aangegeven. Deze *p* en *q* zijn hulpvariabelen, in de vergelijking voor de baan van *S* zullen niet voorkomen.
De lengtes van de loodlijnen uit *P* en *Q* kunnen we gemakkelijk in *a* en *p* of *q* uitdrukken: $\sqrt{a^2-p^2}$ en $\sqrt{a^2-q^2}$.
Omdat gegeven is dat $\overline{PQ} = b$, en de loodlijnen $2b-p-q$ uit elkaar liggen, hebben zo we al direct een verband tussen *p* en *q* gevonden, de *PQ*-vergelijking:

$$PQ: \qquad (2b-p-q)^2 + (\sqrt{a^2-p^2} - \sqrt{a^2-q^2})^2 = b^2$$

$S(x,y)$ heeft afstand *a* tot zowel *P* als *Q*. De afstand van $S(x,y)$ tot de loodlijn uit *P* is $(b+x-p)$. Dat leidt tot een vergelijking met *x*, *y* en *p* wegens de lengte *a* van *PS* en analoog een met *x*, *y* en *q* er in wegens de lengte *a* van *QS*

$$PS: \qquad (\sqrt{a^2-p^2} - y)^2 + (b+x-p)^2 = a^2$$

$$QS: \qquad (\sqrt{a^2-q^2} - y)^2 + (b-x-q)^2 = a^2$$

De *QS*-vergelijking verschilt weinig van de *PS*-vergelijking. De vertaalsleutel is eenvoudig en logisch: verwissel p door q en vervang x door $-x$.
Als we p uit de *PS*-vergelijking als oplossing hebben bevrijd, kunnen we de vertaalsleutel gebruiken om q uit de *QS*-vergelijking vrij te maken en dan beide formules substitueren in de *PQ*-vergelijking: de gezochte *xy*-vergelijking voor de baan van *S* met parameters a en b.
We verzamelen moed en pakken de *PS*-vergelijking aan. Kwadraten uitwerken, de overblijvende wortelvorm links van de '=' zetten en de rest naar rechts brengen, en weer kwadrateren. Een bekend plan, maar we gaan niet als een dolle te keer. Het gaat er om dat we een vergelijking in p vinden en daarom werk en we $(b+x-p)^2$ wél uit als $(b+x)^2+p^2-2p(b+x)$ maar laten we $(b+x)$ als een klontje in de pap aan elkaar plakken.
Er verdampen tijdens het werk heel wat termen in elkaars positieve en negatieve armen; met wat ervaring in deze zaken zie je dat in de *PS*-vergelijking al aankomen. Het resultaat is een vierkantsvergelijking in p. Die laat zich oplossen naar p via de standaardformule. Ja, *It's a lot of dirty paper, with x's and y's and crossed out cancellations and so on.* Het geeft een beetje vertrouwen als na diverse pogingen de tussenresultaten op het kladblaadje eerst uitdijen en zich daarna laten vereenvoudigen. Hier zijn p én q:

$$p = \frac{b+x}{2} \pm \frac{y}{2}\sqrt{\frac{4a^2}{y^2+(b+x)^2}-1} \qquad q = \frac{b-x}{2} \pm \frac{y}{2}\sqrt{\frac{4a^2}{y^2+(b-x)^2}-1}$$

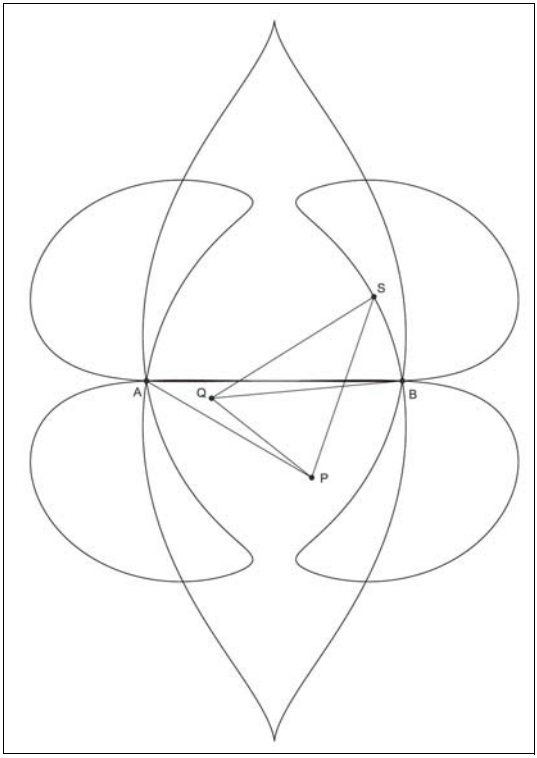
Als we de coördinaten van *S* hebben, dan weten we nu p en q. We hadden het liever andersom gehad! We zien nu wel in, dat als $p+q \neq b$, dat dan niet $y=0$ kan gelden. Maar dat wisten we al uit het synthetische minibewijs. Dat de p- en q-formules het bevestigen, houdt de hoop op resultaat levend.
Nu de vergelijking voor *S(x,y)* opstellen. Moeilijk is dat niet; via copy-paste van de p- en q-formules naar de *PQ*-vergelijking, maken we:

$$\left(2b-\left(\frac{b+x}{2} \pm \frac{y}{2}\sqrt{\frac{4a^2}{y^2+(b+x)^2}-1}\right)-\left(\frac{b-x}{2} \pm \frac{y}{2}\sqrt{\frac{4a^2}{y^2+(b-x)^2}-1}\right)\right)^2$$
$$+$$
$$\sqrt{a^2-\left(\frac{b+x}{2} \pm \frac{y}{2}\sqrt{\frac{4a^2}{y^2+(b+x)^2}-1}\right)^2}-\sqrt{a^2-\left(\frac{b-x}{2} \pm \frac{y}{2}\sqrt{\frac{4a^2}{y^2+(b-x)^2}-1}\right)^2}$$
$$= b^2$$

4. 15 Teleurstelling verwerken en nieuwe koers

Ik twijfel eraan, of nadere uitwerking of vereenvoudiging hier nog wat zal opleveren...

Het valt niet mee uit zo'n forse vergelijking conclusies te trekken over de baan die punt *S* beschrijft. Dat lukte wel heel goed bij de paraboloïde. Daar vonden we met de analytische methode een vergelijking voor de projectie van de doorsnijding van vlak en paraboloïde, en we konder uit de vorm van de vergelijking concluderen: de projectie ís een cirkel.
In veel situaties is het maken van een parametrisering van de kromme geschikter. De keuze van *p* is een poging daartoe: we zouden dan het stelsel van de *PQ*-, *PS*- en *QS*-vergelijking op moeten lossen naar de vorm $x(p) = ..., y(p) = ...$. Dat is hier echter wel lastig...



Er is nog wel iets in het voorgaande dat ander uitzicht biedt. Bij het uitvoeren van de berekeningen werd veel gekwadrateerd en de zorg kan opkomen dat dan allerlei extra oplossingen worden ingevoerd. Dat is zo, maar in dit geval moeten we dat invoeren van oplossingen maar wél doen. Bij de uitvoering in Geogebra zien we ook waarom. Er worden steeds cirkels met cirkels gesneden en we moeten eigenlijk steeds de twéé snijpunten die we vinden gebruiken en bij beide gevonden punten de constructie voortzetten, omdat we niet zeker zijn welke van de twee, of beide gebruikt worden in de mogelijke liggingen van het mechaniek. Zo ontstonden in dit geval in de constructie vier mogelijke punten voor *S* en als we de meetkundige plaatsen van alle vier tekenen krijgen we pas de volledige figuur die bij de vergelijking hoort, te zien. Daaronder zijn ook driehoeken die ontstaan door *PQS* te spiegelen om de basis *PQ*, die zijn niet door beweging bereikbaar vanuit de beginstand van het vlakke mechanisme.
In deze illustratie is *b* wat groter gekozen ten opzichte van *a* en heeft het mecha-

nisme een voor stoommachines ongebruikelijke stand ingenomen. Deze wervelende *deviation from the straight line* mag er wezen!
Geogebra is een geavanceerde analytisch-synthetische ondersteuningsmachine. Het verkennen van de beweging van S is er goed mee mogelijk en is ook niet moeilijk maar wel avontuurlijk en inzicht verschaffend. Hopelijk is vóór het einde van de 21ste eeuw analytische meetkunde met behulp van zulke krachtige middelen op school de standaard, die de beperkingen van onze algebraïsche kunde helpt overstijgen.

Opgave 8. Vervolgonderzoek.
a. Vind een overtuigende, korte synthetische redenering, die laat zien dat S vanuit de uitgangsstand in het midden *onder lijn* AB blijft zolang S de punten A of B niet passeert.
b. Probeer - misschien met behulp van de vorige opgave - inzicht te krijgen in het fenomeen dat S maar weinig van AB afwijkt, als S tussen A en B begint en tussen A en B blijft.

4. 16 Bewijzen met beweging; de *momentane pool*

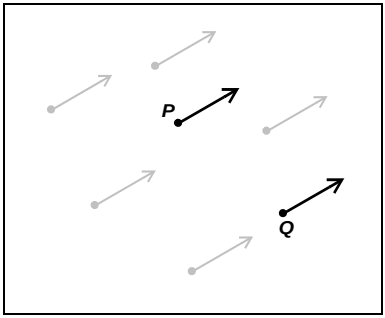
In het voorgaande hebben we meermaals verschillende bewijzen gezien bij dezelfde situatie. Opgemerkt is dat de verschillende bewijzen verschillende verbindingen leggen tussen wat bewezen moet worden en de rest van de wiskundige wereld. Het gaat bij bewijzen dus niet alleen om verificatie, maar om bouwen van een samenhangend netwerk. Nadruk in het voorafgaande lag wel op vrij zuiver synthetische benaderingen en vrij zuiver analytische; de beïnvloeding wederzijds was gering.
Enkele voorbeelden gebruikten nadrukkelijk noties als draaiing, vergroting. In bewijzen die visueel-intuïtief aanspreken zitten vaak transformaties die op het geheel van de betreffende figuur werken, zoals bij de Eulerlijn en het vierkant op de driehoek. Ik pleit hier niet voor een terugkeer van de systematiek van de bewegingsmeetkunde in zijn geheel zoals die in de jaren zestig van de vorige eeuw werd aanbevolen als een alternatief voor de traditionele meetkunde maar wel voor gebruik van de sterke beelden die bewegingen en transformaties en ook het begrip ook snelheid oproepen.
In eerdere voorbeelden was van continue beweging geen sprake. Toch is dat een natuurlijke aanvulling bij de ouderwetse schoolmeetkunde die hoofdzakelijk starre figuren toont. In plaats van de statische *uitdrukking meetkundige plaats* gebruiken velen nu al liever de term *baan van een punt* en helpt Geogebra zulke banen in beeld brengen.
Met een probleem waar intuïtief werken met continue beweging en daarbij horende snelheden succesvol wordt wil ik ook besluiten.
Beweging en snelheid van zich verplaatsende starre objecten horen bij de dage-

lijkse ervaringen en mensen hebben er in vaak heel redelijke intuïties over. Loop je met een koperen staaf van 5 meter lang op de schouder, dan moet je echt goed op de medemens passen als je een bocht maakt, dat wéét je gewoon.Voor zulke intuïties is geen limietbegrip nodig; in het volgende introduceer ik een sleutelbegrip voor de slotopgave ook op een intuïtieve manier zonder exacte bewijzen.

4.16.1 De momentane pool van een schuivend vlak

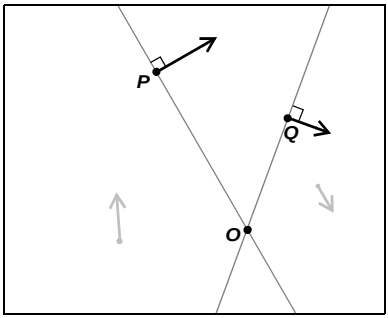
We volgen een een vlakke figuur die zonder vervorming over een vast vlak wordt geschoven. Voor de volledigheid nemen we voor de schuivende figuur wéér een heel vlak. Alle punten van dat vlak bewegen in samenhang.

Beschouw hier in de twee figuren hiernaast punten P en Q als handvaten waarmee het hele vlak bewogen wordt. Uiteraard blijft $\overline{PQ}$ constant. We kijken naar de snelheden van de verschillende punten van het vlak op één moment.



In de bovenste van de twee afgebeelde situaties zijn de snelheden van P en Q gelijk naar richting en grootte. Dan schuift de hele figuur (het hele vlak) op dat moment in één richting. Niets staat dan stil, maar alle punten hebben dan dezelfde snelheid in grootte en richting.

Interessanter is de situatie als de snelheden van P en Q wel in grootte en/of richting verschillen, zoals in deze onderste figuur. Dan zit er ook een draai in de beweging van dat moment. We gaan in proberen te zien, dat de beweging op dat moment dan inderdaad één moment van een echte draaibeweging is en dat er één punt is, dat *momentaan stilstaat*.



Om het inzicht te verscherpen kijken we hier eerst naar het punt P waar een pijltje bij staat dat de richting van de snelheid van P aangeeft. De lijn door P loodrecht op dit pijltje is getekend. Als er al een punt in het schuivende vlak is, dat momentaan stilstaat, dan moet het op die lijn liggen. Voor Q is het net zo. Het enige punt van het schuivende vlak dat stil kan staan is het snijpunt O van die twee lijnen. Nu O bepaald is, zien we dat de beweging van het vlak op dat moment ook de draaiing op dat moment moet zijn, want die draaiing zorgt voor de goede bewegingsrichtingen van P en Q. We zien dat de groottes van de snelheden van P en Q dan ook niet onafhankelijk van elkaar meer gekozen hadden kunnen worden, die groottes verhouden zich als de afstanden tot O.

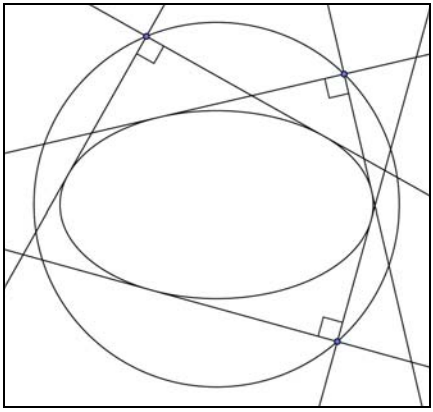
O heet van de beweging op dat moment de *momentane pool*. De momentane snelheden van de ander punten in het vlak kunnen ook gevonden worden. Maar voor ons slotvoorbeeld hebben we alleen de momentane pool nodig van twee punten met verschillende bewegingsrichtingen.

4. 17 De orthoptische cirkel van de ellips; puur analytisch bewijs

De stelling die we als slotprobleem op gaan bewijzen is de stelling van de orthoptische cirkel om de ellips:

De snijpunten van paren onderling loodrechte raaklijnen aan een gegeven ellips
liggen op een cirkel met hetzelfde middelpunt als de ellips.

Als de ellips een cirkel is, is het triviaal. Maar als de ellips langwerpig is, is het bijzonder.



Opgave 9. Werk het volgende zuiver analytische bewijs nader uit.

Zij de ellips gegeven door de vergelijking

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

Een raaklijn aan de cirkel met (door richtingscoëfficiënt *m*) gegeven richting heeft een vergelijking van de gedaante $y = mx + p$. Vind geschikte waarden van *p* door de lijn met de ellips te snijden, en te zorgen dat er maar één snijpunt is. Nu weten we de vergelijkingen van de raaklijnen met richtingscoefficiënt *m*.

Door dit met -1/*m* in plaats van *m* te doen, vinden we ook de raaklijnen die daar loodrecht op staan.

Nu zijn we toe aan het vinden van snijpunten van orthogonale paren raaklijnen. Dat betekent *m* elimineren uit vergelijkingen van loodrechte raaklijnen. Omdat we willen bewijzen dat die snijpunten op een cirkel liggen om de oorsprong, werken we bij het elimineren van *m* slim toe naar $x^2 + y^2$.

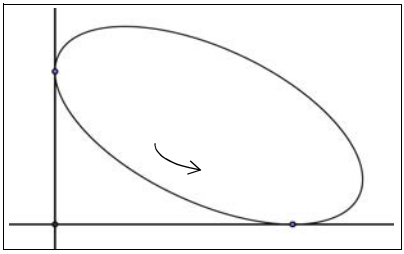
Tip: Werk toe naar $(y - mx)^2 + (my - x)^2 = $.

4. 18 Vast lijnenpaar en draaiende ellips, gemengde technieken

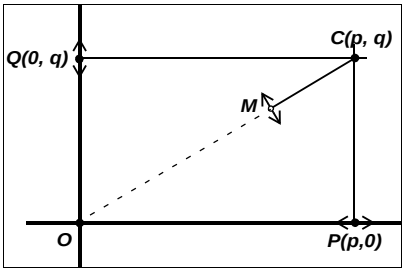
Het hier volgende bewijs voor de stelling van de orthoptische cirkel is eerder opgeschreven ter gelegenheid van het afscheid van Dick Klingens als redacteur van

Euclides voor een herinneringsuitgave in beperkte oplage. Het bewijs gebruikt uiteenlopende technieken; ik zette het in elkaar om de veelzijdigheid van Dick als meetkundige te eren.
Het bewijs mengt analytische en synthetische methodes, een mooi besluit van deze bijdrage. Het analytische deel is veel simpeler dan van het zojuist samengevatte analytische bewijs. Het synthetische deel is direct en rust op het idee van de momentane draaipool. Er gaat nog een omkeerstap aan vooraf.
Het verhaal start met het moment van de inspiratie.

Onlangs fietste ik naar Marken. In de haven kwam de veerboot uit Volendam aan, volgeladen met toeristen. Fiets en ik mochten mee terug naar Volendam in de op kapitein en matroos na lege boot. De rust van de Gouwzee daalde op mij neer. De boot leek stil te liggen en Marken leek traag te draaien en verschuiven.

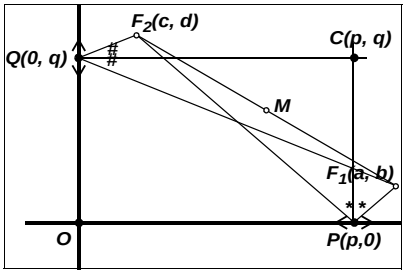


Ik bekijk de situatie van de twee onderling loodrechte raaklijnen aan de ellips nu eens vanuit het snijpunt van de raaklijnen; dat is mijn rustpunt en de O van mijn coördinatenstelsel. De ellips verandert dan steeds van richting ten opzichte van dit stelsel, maar houdt wel contact met beide assen.
Als ik aantoon dat het middelpunt M van de ellips op een vaste cirkel rond O ligt, is $\overline{MO}$ constant en is de stelling van de orthoptische cirkel weer eens bewezen.
In de figuur hiernaast zijn op dit moment van de beweging $P(p, 0)$ en $Q(0, q)$ de raakpunten van de ellips aan de assen. Beschouw P en Q als punten van de ellips, dus als bewegend met het geheel van de ellips en het vlak van de ellips mee. De bewegingsrichtingen van P en Q zijn de richtingen van de coördinaatassen. De *momentane pool* van de beweging is snel gevonden: $C(p, q)$.



Zij nu M het middelpunt van de ellips. Beweegt het vlak met de ellips, dan is het een momentane draai om C en is de bewegingsrichting van M loodrecht op CM. Als M op een vaste cirkel rond O ligt, moet de bewegingsrichting van M ook loodrecht op OM zijn. Daarom wil ik graag bewijzen: M ligt op OC. Als dát zo is, ís de bewegingsrichting van M steeds loodrecht op OM en dat betekent dat M inderdaad op een vaste cirkel om O blijft en is het bewijs rond.
Ik was even bang dat ik nu de ellips zelf precies moest kunnen lokaliseren, maar

dat blijkt niet nodig.
Laat $F_1(a, b)$ het ene brandpunt van de ellips zijn. Met behulp van de spiegeleigenschap van de ellips met raaklijnen OP en OQ vind ik wat dan het tweede brandpunt zou moeten zijn; in de volgende figuur is dat $F_2(c, d)$.



Nu bewijzen we dat het midden M van F_1F_2 op OC ligt! Dit gaat analytisch vrij eenvoudig.
De gelijke hoeken bij P vertellen dat

$$(p - c) : d = (a - p) : b.$$

Daaruit volgt dat

$$b\,(p - c) = d\,(a - p)$$

en dus dat

$$(b + d)\,p = ad + bc.$$

De analoge formule die bij Q hoort kan via de lettervertaling van (a, b, c, d, p, q) naar (d, c, b, a, q, p) worden gevonden; wie dat niet vertrouwt, moet maar even rekenen. Het resultaat is:

$$(a + c)\,q = ad + bc.$$

Uit de gelijkheid

$$(b + d)\,p = (a + c)\,q$$

volgt dat M op OC ligt. Immers,

$$M = ((a + c)/2, (b + d)/2)$$

en we leiden uit

$$(b + d)\,p = (a + c)\,q$$

direct af dat

$$(a + c)/2 : (b + d)/2 = p : q.$$

Bewijs voltooid!

4. 19 Bronnen

[1] Barrau, dr. J. A. (1918), Analytische Meetkunde Deel I - Het Platte Vlak. *Groningen, Noordhoff.*

[2] Bos, Henk J. M. (2001). Redefining geometrical exactness: Descartes' transformation of the early modern concept of construction. *Springer-verlag, New York.*

[3] Descartes, René (1637). La Géométrie. *Tweetalige editie bij Dover Publications INC., New York.*

[4] Dunham, William (1999). Euler, The Master of us All. *The Mathematical Association of America, Dolciani Mathematical Expositions, No. 22.*

[5] Drijvers, P. ed. (2006). Wat a is, dat kun je niet weten. Een pleidooi voor betekenisvolle algebra op school. *Freudenthal Instituut.*

[6] Euclides (ongeveer 300 v. Chr.). De Elementen.
De Engelse vertaling, The Thirteen Books of the Elements, toegelicht door

Thomas Heath is nog steeds verkrijgbaar. *Dover Publications INC., New York.*
Op het web is de tekst, met veel extra's en animaties in Java van David Joyce ook te vinden:
http://aleph0.clarku.edu/~djoyce/java/elements/elements.html.

[7] Goodstein, David L. en Judith R. (1996). Feynman's Lost Lecture. The motion of the planets around the sun. *Vintage, London.*

[8] Hilbert, D. (1899). Grundlagen der Geometrie. Stuttgart: Teubner, 1968

[9] Johnson, Roger A. (1929). Advanced Euclidean Geometry. *Dover Books on Mathematics, 2007.*

[10] Needham, Tristan (1998). Visual complex analysis. *Oxford: Clarendon Press.*
Een fraaie introductie tot de complexe getallen en complexe functietheorie op visueel-intuïtieve wijze.

[11] Kempe, A. B. (1877). How to draw a straight line: a lecture on linkages. *Gutenberg Free ebooks: http://www.gutenberg.org/ebooks/25155*

[12] Kindt, Martin. (2015). Wat te bewijzen was. *Freudenthal Instituut, 2015.* 61 bijdragen over bewijzen, uit de Nieuwe Wiskrant.

[13] Piets, W.A. (1908). Leer boek der Beschrijvende Meetkunde. Twee delen, met atlas. *J. Bootsma, Den Haag.*

[14] Schrek, Dr. D. J. E. (1961). Beknopte Analytische meetkunde. *P. Noordhoff N.V. , Groningen.*

[15] Wells, David (1991).The Penguin dictionary of curious and interesting geometry. *London, Penguin Books.*

5 Hoe bewijs je het priemgetaltweelingvermoeden?

Frits Beukers

Voorwoord

In het voorjaar van 2013 overrompelde de Chinees-Amerikaanse wiskundige Yitang Zhang de wiskundige wereld met de aankondiging van het bewijs dat er een geheel getal A bestaat zó dat er oneindig veel paren gehele getallen $n, n+A$ bestaan die beide priem zijn. Als A gelijk aan 2 zou zijn geweest dan zou dit een bewijs voor het beruchte priemgetaltweeling vermoeden zijn geweest. Dit vermoeden is waarschijnlijk even oud als de getaltheorie zelf. Uit het bewijs van Zhang volgt iets zwakkers, namelijk dat A kleiner is dan zeventig miljoen. Niettemin was het bewijs van Zhang uniek in zijn soort en tot dusver voor onmogelijk gehouden door andere experts in de analytische getaltheorie.

In deze aantekeningen geven we een overzicht van een aantal feiten over priemtweelingen en de ontwikkelingen die leidden tot Zhang's ontdekking en het vervolg erop. Door inspanningen van veel wiskundigen is in de loop van 2013-15 de grens voor A teruggebracht tot 246. We zullen ook proberen het idee van Zhangs bewijs over te brengen. Of dit lukt is nog onzeker, het bewijs is niet helemaal triviaal.

5.1 Inleiding

Een geheel getal > 1 dat alleen zichzelf en 1 als deler heeft noemen we een priemgetal. De rij priemgetallen begint als volgt:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,$$
$$67, 71, 73, 79, 83, 89, 97, 101, 103, 109, 113, 127, 131, 137, 139, 149$$
$$139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,$$
$$211, 223, 227, \ldots$$

Bij het opschrijven van deze rij komt meteen al een stel vragen naar voren. Bijvoorbeeld, gaat deze rij oneindig lang door? Waarschijnlijk wel, maar we moeten er wel een bewijs voor geven. Dat zullen we in dit artikel op twee manieren doen, namelijk een bewijs afkomstig van Euclides en een ander van Euler. Nog een vraag die rijst. Gegeven X, hoeveel priemgetallen $\leq X$ zijn er? Kun je daar een eenvoudige formule voor geven? Dat is wat lastiger te beantwoorden, maar het is in elk geval mogelijk formules te geven die deze aantallen bij grove benadering geven. Dit wordt mogelijk gemaakt door de zogenaamde Priemgetalstelling uit 1899. Nog een vraag: zijn er oneindig veel priemgetallen die op een 1 eindigen? Of een 7? Het antwoord daarop is 'ja' en wordt gegeven door een stelling van Dirichlet uit 1825, die zegt dat elke rij van de vorm

$$a, a+q, a+2q, a+3q, a+4q, \ldots$$

met $a, q \in \mathbb{N}$ en $\text{ggd}(a, q) = 1$, inderdaad oneindig veel priemgetallen bevat. In het bijzonder geldt dit voor de rij $10n + 1$ met $n = 1, 2, 3, \ldots$.

Maar zoals iedereen weet zijn er ook onopgeloste problemen. Bijvoorbeeld het *Goldbachvermoeden* dat zegt dat elk geheel even getal ≥ 4 te schrijven is als som van twee priemgetallen. In de novelle van Dioxiades, 'Uncle Petros and the Goldbach Conjecture', kunnen we lezen hoe iemand tot wanhoop kan worden gedreven door de mislukte pogingen een dergelijk vermoeden aan te tonen. Empirisch bewijsmateriaal is er in overvloed. Het getal 100 is bijvoorbeeld op 6 manieren som van twee priemgetallen en het getal 10000 op 165 manieren. De kunst is echter aan te tonen dat elk even getal op minstens één manier een som van twee priemgetallen is. Dat is tot nog toe niemand gelukt.

Een ander notoir probleem is het *priemtweelingvermoeden*. Merk namelijk op dat

$$(11, 13), (17, 19), (29, 31), (41, 43), (71, 73), (101, 103), \ldots$$

paren opeenvolgende oneven getallen zijn waarvan beide elementen priem zijn. De vraag is of er oneindig veel van bestaan. Waarschijnlijk wel, maar dat is tot dusver nog niet aangetoond. Men heeft wel heel grote priemtweelingen gevonden, bijvoorbeeld

$$3756801695685 \cdot 2^{666669} \pm 1.$$

De enig bekende technieken om dit soort problemen aan te pakken is via de analytische getaltheorie, in het bijzonder de *cirkelmethode* en *zeefmethoden*. Dit zijn lastige technieken die heel veel gebruik maken van slimme afschattingen en resultaten uit de Fouriertheorie en complexe functietheorie.

De vooruitgang in concrete resultaten is over het algemeen heel langzaam. Maar soms zijn er verrassingen. Zo lieten bijvoorbeeld Terence Tao en Ben Green in 2008 zien dat er in de rij priemgetallen eindige rekenkundige rijen kunnen voorkomen van elke gekozen lengte. De tot nu toe (februari 2015) langst bekende rekenkundige rij heeft lengte 26 en wordt gegeven door

$$161004359399459161 + 47715109 \cdot 223092870 \cdot n \quad \text{voor } n = 0, 1 \ldots, 25.$$

Een andere spectaculaire ontwikkeling is nog recenter. In het voorjaar van 2013 kondigde de Chinees-Amerikaanse wiskunde Yitang Zhang aan dat er een getal A bestaat zó dat er oneindig veel paren priemgetallen van de vorm $n, n + A$ zijn. Als A gelijk zou zijn aan 2, zou dit een bewijs van het priemgetaltweelingvermoeden hebben betekend. Zhang kon alleen maar aantonen dat $A < 70.000.000$. Maar zelfs dit resultaat is uniek in zijn soort en eigenlijk door niemand voorzien. Het artikel, dat Zhang bij het prestigieuze Annals of Mathematics indiende, werd al vrij snel door de referees goedgekeurd en gepubliceerd.

Het verhaal rond deze doorbraak is een bijzondere. Wiskundige onderzoekers worden geacht hun meest creatieve werk rond hun 30e te produceren. Zhang was 58 jaar oud en bovendien had hij tot dan toe weinig gepubliceerd op wiskundegebied. Op de Nederlandse Wikipedia vind je een uitgebreide beschrijving van de levensloop van Zhang. Een interview kun je vinden in een artikel uit de New Yorker, als dat er nog staat,

`http://www.newyorker.com/magazine/2015/02/02/pursuit-beauty`

De grens van 70 miljoen in Zhang's stelling is een gevolg van de methode die hij gebruikte. Het was toen al duidelijk dat met een wat voorzichtiger benadering deze waarde wel kleiner gemaakt zou kunnen worden. En dat is precies wat gebeurde. Een paar weken na Zhang's publicatie stelde Terence Tao een zogenaamd Polymath project voor. Een publiek project via internet waar in principe iedereen aan kon bijdragen. Het eerste deel van het project werd afgesloten met een grens van 4680. Tijdens dit project kwam de jonge Canadese postdoc James Maynard met een iets andere aanpak die eenvoudiger bleek te zijn en ook nog eens betere grenzen opleverde. Dit werd deel twee van het project dat uiteindelijk afgesloten werd met een grens van 246. Voor een overzicht van deze historie en de huidige stand van zaken, zie

`http://michaelnielsen.org/polymath1/`
`index.php?title=Bounded_gaps_between_primes`

Zoals het er nu naar uitziet zullen er nieuwe ideeën nodig zijn om de grens 2 van het priemtweelingvermoeden te bereiken.

Het nadeel van veel recente opzienbare ontwikkelingen in de wiskunde is, dat de details vaak te ingewikkeld en specialistisch zijn voor een breder publiek van niet-ingewijden. Het aantal wiskundigen dat bijvoorbeeld de details van het bewijs van de laatste stelling van Fermat kent is zeer beperkt. De reden is dat je eerst enkele jaren moet wijden aan het bestuderen van onderwerpen als modulaire vormen, galoisrepresentaties, etc, die de basis vormen van het bewijs. Het prettige van Maynard's bewijs is dat, als je bereid bent een 'black box' te accepteren, de afleiding relatief weinig voorkennis vereist, maar wel een flinke portie technische vaardigheid en uithoudingsvermogen. In principe zou een goede derdejaars wiskundestudent het bewijs moeten kunnen volgen, met eventueel wat begeleiding. En dit is inderdaad wat er gebeurd is, Ilja Nelen, vorig jaar nog bachelorstudent, heeft Maynard's bewijs als onderwerp voor zijn bachelorscriptie gehad.

Gesterkt door deze ervaring zal ik aan het eind van deze tekst heel kort een indruk geven van de ingredienten van het bewijs van Maynard's resultaat. Maar voor het zover is geven we een inleiding in wat we weten van priemgetaltweelingen, hetgeen hopelijk wat lichtere kost vormt.

5.2 Priemgetallen tellen

In deze paragraaf kijken we naar de oneindigheid van de verzameling priemgetallen en hoe vaak ze voorkomen onder de natuurlijke getallen (dat zijn gehele getallen ≥ 1).

Stelling 5.2.1 (Euclides)**.** *Bij elk natuurlijk getal N bestaat er een priemgetal p dat groter is dan N.*

Hieruit volgt meteen dat er oneindig veel priemgetallen zijn. Je kunt bijvoorbeeld voor N de getallen $10, 100, 1000, \ldots$ kiezen.

Bewijs: Kijk naar het getal $N!+1$, waarin $N!$ staat voor het product van alle getallen van 1 tot en met N. Deze heeft een priemdeler. Noem deze p. Stel dat $p \leq N$. Dan is p ook een deler van $N!$ Maar een priemgetal kan niet twee opeenvolgende getallen delen. Dus $p \leq N$ kan niet gelden. Conclusie: $p > N$.

□

Hier is een variant die je zelf kunt proberen aan te tonen.

Opgave 5.2.2. *Bewijs dat er oneindig veel priemgetallen van de vorm $4k-1$ zijn. Hint: gebruik het feit dat het product van getallen van de vorm $4m+1$ weer van deze vorm is.*

Hier is een wat sterker resultaat.

Stelling 5.2.3 (Euler)**.** *De oneindige reeks*

$$\sum_{p \text{ priem}} \frac{1}{p}$$

is divergent. Dat wil zeggen als je de inverse priemgetallen $1/2, 1/3, 1/5, 1/7, 1/11, \ldots$ achtereenvolgens bij elkaar optelt, dan gaat de rij gevonden waarden naar oneindig toe.

Uiteraard volgt hieruit dat er oneindig veel priemgetallen bestaan. Het bewijs hiervan is wat lastiger. Het is misschien wel bekend dat de som van de inverse natuurlijke getallen divergent is. Dus

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots=\infty$$

We noemen dit de harmonische reeks. Om de divergentie in te zien breken we de reeks op in stukjes waarbij de som van elk stukje $> 1/2$ is, als volgt:

$$\begin{aligned} \frac{1}{3}+\frac{1}{4} &> 2\times\frac{1}{4}=\frac{1}{2} \\ \frac{1}{5}+\cdots+\frac{1}{8} &> 4\times\frac{1}{8}=\frac{1}{2} \\ \frac{1}{9}+\cdots+\frac{1}{16} &> 8\times\frac{1}{16}=\frac{1}{2} \end{aligned}$$

etcetera. De som van deze waarden $1/2$ gaat naar oneindig. Dit bewijs werd al in de 14e eeuw gevonden door Nicole d'Oresme.

We bewijzen nu Euler's stelling.

Bewijs: We kiezen N en merken allereerst op dat

$$\prod_{p\le N}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) > \frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{N}, \tag{5.1}$$

waarin het product over de priemgetallen $p \le N$ loopt. Bij het wegwerken van de haakjes uit het product moet je uit elke factor een term nemen en

vervolgens die termen vermenigvuldigen. Als we bijvoorbeeld de termen $1/2, 1/3$, en 1 voor de andere factoren neemt, krijg je $1/6$. Dit wordt precies de term $1/6$ rechts. Op deze manier zie je dat het product links alle inversen van gehele getallen geeft, die samengesteld zijn met priemfactoren $\leq N$. Dat zijn in ieder geval 1 tot en met N. Vandaar het ongelijheidteken.

Beschouw nu de volgende ongelijkheid

$$\prod_{p\leq N}\left(1+\frac{1}{p}\right)^2 > \prod_{p\leq N}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right). \tag{5.2}$$

Deze volgt door in elke factor de ongelijkheid $(1+x)^2 > 1+x+x^2+x^3+\cdots$ voor $x \leq 1/2$ te gebruiken. Dit is een kleine opgave, die laat ik aan de lezer over. Nu nog een derde ongelijkheid,

$$\sum_{p\leq N}\frac{1}{p} > \sum_{p\leq N}\log\left(1+\frac{1}{p}\right) = \log\prod_{p\leq N}\left(1+\frac{1}{p}\right). \tag{5.3}$$

Deze volgt uit het feit dat we in elke term $x > \log(1+x)$ kunnen gebruiken voor $x > 0$ (NB: de log hier is de ln op school).

In de ongelijkheid (5.1) staat rechts de harmonische reeks. Die gaat naar oneindig als $N \to \infty$. Uit ongelijkheid (5.1) volgt dat ook

$$\prod_{p\leq N}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)$$

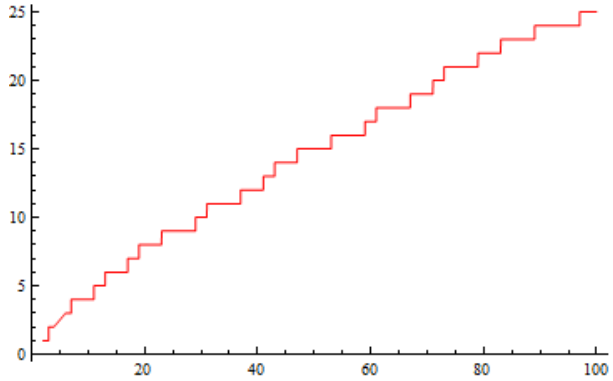
naar oneindig gaat als $N \to \infty$. Uit de ongelijkheid (5.2) concluderen we vervolgens dat $\prod_{p\leq N}\left(1+\frac{1}{p}\right)$ naar oneindig gaat als $N \to \infty$. Tenslotte, met ongelijkheid (5.3) concluderen we dat $\sum_{p\leq N}\frac{1}{p}$ naar oneindig gaat als $N \to \infty$.

□

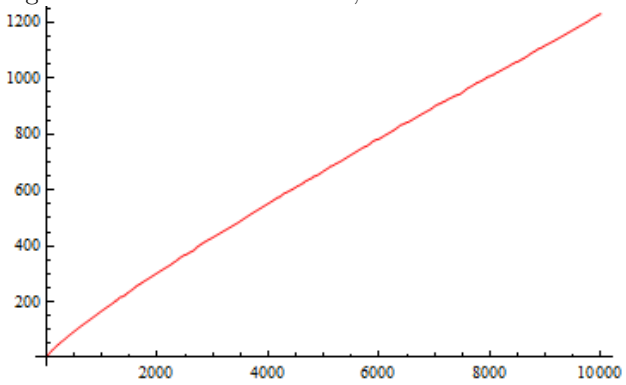
We gaan nu priemgetallen tellen en definieren de zogenaamde priemgetaltelfunctie

$$\pi(x) = \#\{p \leq x |\ p \text{ priem}\},$$

waarin we 'aantal' met het symbool # aangeven. Hier is een grafiek van $\pi(x)$ voor $x \leq 100$.



Hierin zien we duidelijk de stapjes die gemaakt worden als we met x een priemgetal passeren. Deze onregelmatigheden verdwijnen (op het oog) als we een wat groter domein voor x kiezen,



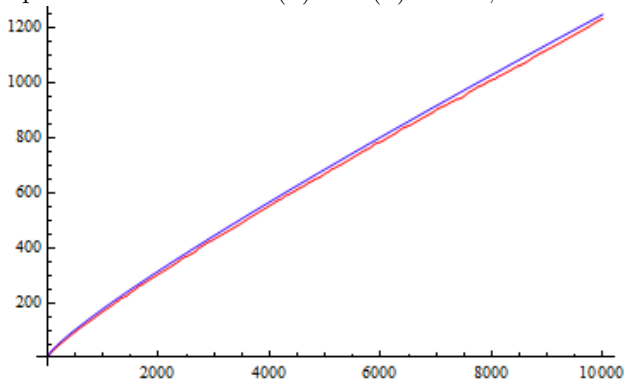
De grafiek is nu een mooie vloeiende figuur geworden en men kan zich afvragen of er een eenvoudige formule bestaat om deze grafiek (bij benadering) te beschrijven. Hier is veel over gespeculeerd, maar het was Gauss die een duidelijk heuristisch argument gaf. Kies X heel groot en Δ klein ten opzichte daarvan. Het principe van Gauss zegt dat het aantal priemgetallen in het interval $[X, X + \Delta]$ ongeveer gelijk is aan $\Delta / \log X$. Met andere woorden, de gemiddelde dichtheid van de priemgetallen in de buurt van X is $1/\log X$. Ter ondersteuning hiervan berekende Gauss een aantal tabellen zoals het onderstaande. Daarin is $\Delta = 10^5$ genomen en met $s(x)$ geven we het aantal priemgetallen in $[x, x + 10^5]$ aan.

x	$s(x)$	$10^5/\log(x)$
10^8	5411	5428
10^9	4832	4825
10^{10}	4306	4342
10^{11}	4019	3948
10^{12}	3614	3619
10^{13}	3382	3340
10^{14}	3045	3102
10^{15}	2804	2895

Merk op dat de getallen in de tweede en derde kolom meestal in hun eerste twee cijfers overeenkomen. Als we aannemen dat de dichtheid van de priemgetallen in de buurt van X gelijk is aan $1/\log X$, dan is het aantal priemgetallen $\leq x$ gelijk aan de som van alle dichtheden van, zeg, 2 tot en met X en dus

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}.$$

Hier is een plot van de functies $\pi(x)$ en $\mathrm{li}(x)$ samen,



In deze plot geldt dat $\pi(x) < \mathrm{li}(x)$, maar dat is niet altijd zo. Het blijkt namelijk dat $\pi(x) - \mathrm{li}(x)$ oneindig vaak van teken wisselt. Voor welke x dat voor het eerst gebeurd weet men echter niet.

Dat $\pi(x)$ en $\mathrm{li}(x)$ inderdaad dicht bij elkaar liggen wordt bevestigd door de *priemgetalstelling*:

Stelling 5.2.4 (Hadamard, De la Vallée-Poussin, 1899)**.** *De verhouding van* $\pi(x)$ *en* $\mathrm{li}(x)$ *gaat naar* 1 *als* x *naar oneindig gaat.*

Het blijkt dat $\mathrm{li}(x)$ redelijk in de buurt ligt van $x/\log x$. Dit mag je zelf uitwerken in de volgende opgave.

Opgave 5.2.5. *Bewijs dat de verhouding van* $\mathrm{li}(x)$ *en* $x/\log x$ *naar* 1 *gaat als* $x \to \infty$.

5.3 Priemtweelingen tellen

We voeren nu een telfunctie voor priemtweelingen in:

$$\pi_2(x) := \#\{n \leq x | n \text{ en } n+2 \text{ priem}\}.$$

Het priemgetaltweelingvermoeden komt dus neer op $\pi_2(x) \to \infty$ als $x \to \infty$.

Om een grof idee van $\pi_2(x)$ te krijgen herhalen we het idee van Gauss. Kies X heel groot en Δ iets kleiner. We vragen ons af hoeveel priemtweelingen er in het interval $[X, X+\Delta]$ voorkomen. We laten daartoe n van X tot $X+\Delta-1$ lopen en bepalen de kans dat zowel n als $n+2$ priem zijn. Als deze kansen onafhankelijk zouden zijn is dat ongeveer $1/(\log X)^2$ waarmee het aantal priemparen op ongeveer $\Delta/(\log X)^2$ komt. Helaas is de kans dat $n+2$ priem is enigszins afhankelijk van die van n. Als bijvoorbeeld toevallig $n \equiv 1 (\mathrm{mod}\ 3)$, en $n > 1$, dan is $n+2$ zeker geen priem, want deelbaar door 3.

Hier is een suggestie om dit probleem te omzeilen. Kies een klein priemgetal p en kijk naar alle n in $[X, X+\Delta]$ die niet deelbaar door p zijn. Dat zijn ongeveer $\left(1-\frac{1}{p}\right)\Delta$ getallen. Het aantal priemgetallen in deze verzameling is nog steeds $\Delta/\log X$. De kans dat een n uit onze beperktere verzameling priem is, is daarmee $\left(1-\frac{1}{p}\right)^{-1}\frac{1}{\log X}$.

Kijk nu naar alle paren $n, n+2$ zodat n noch $n+2$ deelbaar is door p. Dit zijn ongeveer $\left(1-\frac{2}{p}\right)\Delta$ paren als p oneven is. Als p even is (dus $p=2$), moeten we $\frac{2}{p}$ vervangen door $\frac{1}{p}$ (waarom zou dat moeten?). De kans dat van deze $\left(1-\frac{2}{p}\right)\Delta$ paren zowel n als $n+2$ priem is nu $\left(1-\frac{1}{p}\right)^{-2}\frac{1}{(\log X)^2}$. Dit moeten we voor alle p doen en vinden dat het aantal priemgetaltweelingen tussen X en $X+\Delta$ gelijk is aan

$$C_2 \frac{\Delta}{(\log X)^2} \quad \text{met} \quad C_2 = 2 \times \prod_{\substack{p \text{ oneven} \\ \text{priem}}} \frac{(1-2/p)}{(1-1/p)^2} \approx 1.32.$$

Dit geeft aanleiding tot het volgende vermoeden.

Vermoeden 5.3.1. *Definieer*

$$\mathrm{li}_2(x) := C_2 \int_2^x \frac{dt}{(\log t)^2}.$$

Dan gaat de verhouding van $\mathrm{li}_2(x)$ *en* $\pi_2(x)$ *naar* 1 *als* $x \to \infty$.

Om in te zien hoe goed deze benadering is geven we een tabel. Hierin is $s_2(x)$ gelijk aan het aantal priemtweelingen in $x, x + 10^5$.

x	$s_2(x)$	$C_2 \times 10^5/(\log x)^2$
10^8	377	389
10^9	341	307
10^{10}	262	249
10^{11}	182	205
10^{12}	171	172
10^{13}	142	147
10^{14}	123	127
10^{15}	117	110

Dit lijkt goed te gaan. Helaas is er echter weinig bewezen. Met behulp van *zeefmethoden* heeft men bewezen dat een constante $C > 0$ bestaat zó dat $\pi_2(x) < C \cdot \mathrm{li}_2(x)$ geldt als x groot genoeg is. Een gevolg van deze bovengrens is de volgende stelling.

Stelling 5.3.2 (V.Brun, 1919)**.** *De oneindige som*

$$\sum_{\substack{p \text{ en } p+2 \\ \text{priem}}} \frac{1}{p}$$

convergeert.

Dit is het eerste niet-triviale resultaat op het gebied van priemtweelingen. Voor we verder gaan noem ik nog een ander resultaat. Een getal n heet *bijna priem* als het ofwel priem is, ofwel een product van twee priemgetallen.

Stelling 5.3.3 (Chen, Jing-Run, 1973)**.** *Er bestaan oneindig veel priemgetallen p zó dat $p+2$ een bijna priem is.*

Dit was destijds een opzienbarend resultaat en de Chinese posterijen hebben een postzegel aan het werk van Chen gewijd. Die zie je hierboven.

5.4 Generalisaties

In plaats van priemtweelingen kunnen we ook naar andere paren kijken. Paren priemgetallen van de vorm

- $n, n+2$ heten priemtweelingen
- $n, n+4$ heten priemneven/nichten
- $n, n+6$ heten sexy paren, etc

Ook kunnen we drietallen nemen. Bijvoorbeeld $n, n+2, n+4$.

Opgave 5.4.1. *Bewijs dat minstens één van de getallen $n, n+2, n+4$ deelbaar is door 3. Bewijs vervolgens dat de enige priemdrieling van deze vorm gegeven wordt door $n = 3$.*

Kies nu een willekeurige rij van k gehele getallen $0 = a_1 < a_2 < \cdots < a_k$. We beschouwen k-tupels $n + a_1, n + a_2, \ldots, n + a_k$ en vragen ons af of er oneindig veel n bestaan zó dat elk van deze getallen priem is.

We noemen een priemgetal p een obstructie voor rijen van het type $n + a_1, \ldots, n + a_k$ als voor elke geheel getal n minstens één van de getallen $n + a_1, n + a_2, \ldots, n + a_k$ deelbaar is door p. We zagen net dat $p = 3$ een obstructie is voor $n, n+2, n+4$.

Opgave 5.4.2. *Stel dat p een obstructie is. Bewijs dat $p < a_k$. Bewijs vervolgens dat rijen van de vorm $n, n+2, n+6$ geen obstructie hebben.*

We noemen de rij $a_1 < a_2, \cdots < a_k$ *toelaatbaar* als rijen van het type $n + a_1, \ldots, n + a_k$ geen enkele obstructie hebben.

Opgave 5.4.3. *Geef meer voorbeelden van toelaatbare rijen van lengte 3. Bewijs dat er bij elke $k \in \mathbb{N}$ een toelaatbare rij van lengte k bestaat.*

Hier is een generalisatie van het priemtweelingvermoeden.

Vermoeden 5.4.4. *Stel dat $a_1 < a_2 < \cdots < a_k$ toelaatbaar is. Dan zijn er oneindig veel n zó dat $n + a_1, n + a_2, \ldots, n + a_k$ allen priem zijn.*

Natuurlijk zijn we nog een heel eind verwijderd van het bewijs van een dergelijk vermoeden, maar het gebruik van toelaatbare rijen speelt wel een belangrijke rol in het werk van Zhang en Maynard.

5.5 Gaten vullen

We gaan langzamerhand naar de vraag toe hoe klein de afstand tussen opeenvolgende priemgetallen kan zijn. Daartoe noteren we de rij priemgetallen met $p_1 < p_2 < p_3 < \cdots < p_n < \cdots$ In het bijzonder, $p_1 = 2, p_2 = 3$, etc.

Vraag: Kies $c > 0$. Kunnen we aantonen dat er oneindig veel n zó dat

$$p_{n+1} - p_n < c \cdot \log p_n \ ?$$

Om te illustreren hoe lastig deze vraag is, geven we een chronologisch overzicht van de bewezen resultaten op dit gebied.

1. Als $c > 1$ dan is het antwoord 'ja'. Dit is een gevolg van de priemgetalstelling. Dit is een (behoorlijk lastige) opgave voor de lezer.
2. Ja, een dergelijke c bestaat met $c \leq 1$ (Erdös, 1940). Dit is geen opgave voor de lezer meer, maar een diep resultaat.
3. Ja, voor elke $c \geq 1/2$ (Bombieri-Davenport, 1966).
4. Ja, voor elke $c \geq 1/4$ (Maier, 1988).
5. Ja, voor elke $c > 0$ (Goldston-Yilderim-Pintz, 2005).

We zien dat de ontwikkeling heel langzaam gaat, en dat geeft aan dat het een buitengewoon lastige vraag is. Het laatste resultaat van Goldston, Yilderim en Pintz uit 2005 was zelfs een onverwachte doorbraak. Er geldt nog iets meer.

Stelling 5.5.1 (GYP, 2005)**.** *Voor elke $\epsilon > 0$ heeft de ongelijkheid*

$$p_{n+1} - p_n < (\log p_n)^{1/2+\epsilon}$$

oneindig veel oplossingen.

Na het bekend worden van deze stelling had men enige tijd hoop dat er een mogelijk bewijs richting priemtweelingen in zat. Helaas, na een aanvankelijk optimisme werd het weer stil rond deze kwestie. Totdat in 2013 een volgende doorbraak plaatsvond.

Stelling 5.5.2 (Yitang Zhang, 2013)**.**
Er zijn oneindig veel n zó dat

$$p_{n+1} - p_n < 70.000.000$$

Zoals in de inleiding gezegd, werd dit resultaat al snel vereenvoudigd en verbeterd door Maynard. In de laatste paragraaf geven we een overzicht van de stappen van dit alternatieve bewijs van Maynard.

5.6 Het bewijs van Maynard

De techniek is gebaseerd op telresultaten van priemgetallen in een rekenkundige rij. In de inleiding hebben we de stelling van Dirichlet genoemd, die zegt dat als $\text{ggd}(a, q) = 1$, dan bevat de rij $a, a + q, a + 2q, a + 3q, \ldots$ oneindig veel priemgetallen. Het aantal priemgetallen $\leq x$ in deze rij geven we aan met $\pi(x, a, q)$. De verwachting is dat alle restklassen a modulo q die in aanmerking komen ongeveer evenveel priemgetallen zullen bevatten. Gegeven q dan geven we het aantal getallen $0 < a \leq q$ met $\text{ggd}(a, q) = 1$ aan

met $\phi(q)$, de Euler ϕ-functie. Bijvoorbeeld $\phi(4) = 2, \phi(5) = 4, \phi(6) = 2, \ldots$ We verwachten dat voor gegeven q de $\phi(q)$ functies $\pi(x, a, q)$ allen ongeveer even met x zullen groeien. Dit werd voor het eerst quantitatief gemaakt in de volgende stelling.

Stelling 5.6.1 (Siegel-Walfisz, 1936)**.** *Bij elke $A > 1$ bestaat een $C > 0$ zó dat voor alle x,*

$$\left|\pi(x, a, q) - \frac{\pi(x)}{\phi(q)}\right| < C \ \frac{x}{(\log x)^A}.$$

Omdat $\pi(x)$ ongeveer gelijk is aan $x/\log x$ zien we in het bijzonder dat de verhouding tussen $\pi(x, a, q)$ en $\pi(x)/\phi(q)$ naar 1 gaat als $x \to \infty$. Met andere woorden, de priemgetallen zijn ongeveer gelijk verdeeld over de restklassen $a (\mathrm{mod}\ q)$.

Het blijkt dat voor het merendeel van de x-waarden het verschil tussen $\pi(x, a, q)$ en $\pi(x)/\phi(q)$ veel kleiner is dan dat gegeven door de stelling van Siegel-Walfisz. Dit wordt geaccenteerd door de volgende stelling die simpelweg een heleboel verschillen by elkaar optelt als we q over een grote range laten lopen.

Stelling 5.6.2 (Bombieri-Vinogradov, 1965)**.** *Bij elke $A > 1$ en elke $\theta < 1/2$ bestaat er een $C > 0$ zó dat voor elke x,*

$$\sum_{q \le x^\theta} \max_{\mathrm{ggd}(a,q)=1} \left|\pi(x, a, q) - \frac{\pi(x)}{\phi(q)}\right| < C \ \frac{x}{(\log x)^A}.$$

Dit is een stelling die met de zogenaamde *grote zeef* bewezen kan worden. Het is het uitgangspunt voor het werk van Goldston, Yilderim, Pintz. Om hun werk te verbeteren richting priemgetaltweelingen zou je eigenlijk de stelling van Bombieri-Vinogradov moeten hebben met een waarde van $\theta > 1/2$. Ondanks alle pogingen in die richting is het nog niemand gelukt een dergelijk resultaat te bewijzen. De bijdrage van Zhang bestaat er uit dat hij een iets andere, verfijnde versie van Bombieri-Vinogradov ontwierp waarbij $\theta > 1/2$ is. Dit was een onverwachte wending die niemand had voorzien. De alternatieve versie van Zhang is behoorlijk technisch en niet makkelijk uit te leggen. Het is daarom prettig dat Maynard met een heel ander idee kwam waarvoor alleen de stelling van Bombieri-Vinogradov voldoende is. We kunnen deze stelling nu als een soort 'black box' gebruiken in de volgende schets van Maynard's aanpak.

Met $\chi_{\mathbb{P}}(n)$ geven we de karakteristieke functie aan van de priemgetallen. Dat wil zeggen, $\chi_{\mathbb{P}}(n) = 1$ als n priem is en 0 indien niet. Zij $a_1, \ldots, a_k$

een toelaatbare rij en kies $\rho > 1$. Beschouw voor elke $N \in \mathbb{N}$,

$$S(N,\rho) = \sum_{N \le n \le 2N} w(n) \left(-\rho + \sum_{i=1}^{k} \chi_{\mathbb{P}}(n+a_i) \right) \tag{5.4}$$

met geschikt gekozen gewichten $w(n) > 0$ (die kiezen we later). Stel dat we kunnen aantonen dat $S(N,\rho) > 0$ voor N groot genoeg. Dan bestaat er een n met $N \le n \le 2N$ zó dat $-\rho + \sum_{i=1}^{k} \chi_{\mathbb{P}}(n+a_i) > 0$. Omdat $\rho > 1$ moeten er zich minstens twee priemgetallen in de rij $n+a_1, \ldots, n+a_k$ bevinden om de ongelijkheid > 0 te krijgen. Dus hebben we twee priemgetallen met verschil $\le a_k - a_1$ gevonden. Omdat N willekeurig groot kan worden gekozen vinden we op deze wijze oneindig veel paren met afstand $\le a_k - a_1$.

We gaan nu geschikte gewichten $w(n)$ in (5.4) kiezen. Goldston, Yilderim en Pintz kozen $\delta > 0, R = N^{1/2-\delta}$ en vervolgens

$$w(n) = \left(\sum_{d \mid (n+a_1)\cdots(n+a_k), d \le R} \lambda(d) \right)^2$$

waarin

$$\lambda(d) := \mu(d) \left(\frac{\log d}{\log R} \right)^{k+l}$$

voor een geschikte l. Hier is $\mu(d)$ de zogenaamde Möbius μ-functie die gedefinieerd wordt door $\mu(d) = (-1)^t$ als $d = p_1 \ldots p_t$ en 0 als d deelbaar is door een kwadraat > 1.

Zoals we reeds gemeld leek deze keuze van $w(n)$ zeer effectief in 2005, maar niet effectief genoeg richting priemtweelingen. James Maynard bedacht een andere gewichtsfunctie, namelijk

$$w(n) = \left(\sum_{d_1 \mid (n+a_1), \ldots, d_k \mid (n+a_k), d_1 \cdots d_k \le R} \lambda(d_1, \ldots, d_k) \right)^2$$

met $R = N^{1/2-\delta}$ en

$$\lambda(d_1, \ldots, d_k) := \prod_{i=1}^{k} \mu(d_i) d_i \sum_{\substack{r_1, \ldots, r_k \\ d_i \mid r_i}} \prod_{i=1}^{k} \frac{1}{\phi(r_i)} F\left(\frac{\log r_1}{\log R}, \ldots, \frac{\log r_k}{\log R} \right)$$

voor een slim gekozen functie $F(x_1, \ldots, x_k)$ op de verzameling in $\mathbb{R}^k$ die voldoet aan de ongelijkheden $x_i \ge 0$ voor $i = 1, \ldots, k$ en $x_1 + \cdots + x_k \le 1$. Met deze keuze krijgen we de volgende stelling.

Stelling 5.6.3 (James Maynard, 2014)**.** *Er zijn oneindig veel n zó dat*

$$p_{n+1} - p_n < 600.$$

Hier volgt een kort overzicht van het bewijs, zonder al te veel op de details in te gaan. We hadden gedefinieerd

$$S(N,\rho) = \sum_{N \le n \le 2N} w(n) \left(-\rho + \sum_{i=1}^{k} \chi_{\mathbb{P}}(n + a_i) \right)$$

hetgeen we afkorten tot $S(N,\rho) = -\rho S_2(N) + S_1(N)$. Om ervoor te zorgen dat $S(N,\rho) > 0$ wordt moeten we ervoor zorgen dat er een $\rho > 1$ bestaat zó dat $S_1(N)/S_2(N) > \rho$ als N groot genoeg is. Door gebruik te maken van de gewichtsfunctie van Maynard en de stelling van Bombieri-Vinogradov kan men aantonen dat

$$\frac{S_1(N)}{S_2(N)} = (1/2 - \delta + o(1)) \frac{\sum_{m=1}^{k} J_k^{(m)}(F)}{I_k(F)}.$$

waarin

$$I_k = \int_0^1 \cdots \int_0^1 (F(t_1, \ldots, t_k)^2 dt_1 \cdots dt_k$$

en

$$J_k^{(m)} = \int_0^1 \cdots \int_0^1 \left(\int_0^1 F(t_1, \ldots, t_k) dt_m \right)^2 dt_1 \cdots dt_{m-1} dt_{m+1} \cdots dt_k.$$

Met $o(1)$ bedoelen we een functie die naar 0 gaat als $N \to \infty$. Om het bewijs af te maken is het zaak een functie F te vinden zó dat

$$\frac{\sum_{m=1}^{k} J_k^{(m)}(F)}{I_k(F)} > 2.$$

Alleen dan kunnen we, door δ klein genoeg te kiezen en $\rho > 1$ dicht genoeg bij 1, ervoor zorgen dat $S_1(N)/S_2(N) > \rho$ als N voldoende groot is. Het vinden van een geschikte F is een subtiel optimalisatieprobleem en het is verrassend dat het inderdaad mogelijk is. We moeten daarvoor wel zoeken onder functies in minstens 105 variabelen. Dat wil zeggen, $k \geq 105$. Hier is een toelaatbare rij van lengte 105,

$0, 10, 12, 24, 28, 30, 34, 42, 48, 52, 54, 64, 70, 72, 78, 82, 90, 94,$
$100, 112, 114, 118, 120, 124, 132, 138, 148, 154, 168, 174, 178, 180,$
$184, 190, 192, 202, 204, 208, 220, 222, 232, 234, 250, 252, 258, 262, 264,$
$268, 280, 288, 294, 300, 310, 322, 324, 328, 330, 334, 342, 352, 358, 360,$
$364, 372, 378, 384, 390, 394, 400, 402, 408, 412, 418, 420, 430, 432, 442,$
$444, 450, 454, 462, 468, 472, 478, 484, 490, 492, 498, 504, 510, 528, 532,$
$534, 538, 544, 558, 562, 570, 574, 580, 582, 588, 594, 598, 600.$

Merk op dat $a_{105} - a_1 = 600$ en dat verklaart de grens in de stelling van Maynard. Latere verbeteringen hebben ervoor gezorgd dat de grens op 246 kwam. Dat is nu (juni 2015) het record.

Door k nog groter te kiezen kunnen we

$$\frac{\sum_{m=1}^{k} J_k^{(m)}(F)}{I_k(F)}$$

zo groot maken als we willen. Gevolg,

Stelling 5.6.4 (Zhang, Maynard)**.** *Stel $m \in \mathbb{N}$. Dan bestaat er een C_m zó dat*

$$p_{n+m} - p_n < C_m$$

voor oneindig veel n.

Met andere woorden, by elke $m \in \mathbb{N}$ bestaat een getal C_m zó dat er oneindig veel intervallen met lengte C_m zijn die $m + 1$ priemgetallen bevatten.

6 Oeps, foutje!
Jan Brandts

6.1 Inleiding

Er zullen maar weinig mensen echt warm lopen voor de analyse van door rekenmachines gemaakte afrondfouten, en van pogingen vanuit de wiskundige gemeenschap om het niet-exact rekenen tot wetenschap te verheffen. De corresponderende kretologie, gedomineerd door termen als floating-point getallen, conditionering, en stabiliteit, maakt het er ook al niet veel aantrekkelijker op. Daarnaast zal menigeen met ingehouden leedvermaak kennis nemen van alweer een ramp die zich kon voltrekken doordat de verantwoordelijke rekenaars zich niet aan "de regels" hielden.

En toch. Eenieder vergaapt zich aan de mooiste plaatjes van fractals die blijkbaar uitgerekend kunnen worden, men vindt Chaostheorie een interessant klinkend vakgebied, en we willen allemaal dat het weer goed wordt voorspeld, in het bijzonder als er goed weer wordt voorspeld. Het credo lijkt derhalve: "We willen niet weten hoe het werkt, als het maar werkt!"

U zult begrijpen dat dit eigenlijk niet helemaal fair is jegens de nijvere bij die in de afgelopen decennia deze aspecten van de wiskunde heeft helpen ontwikkelen. Vandaar dat we een poging zullen doen om wat inzicht te verschaffen in de problemen die het rekenen met een machine met zich meebrengt. Voorkennis is nauwelijks vereist, slechts een open blik en een onbevooroordeelde geest. En wie weet wordt u verrast!

6.2 Een afschrikwekkend rekenresultaat

Laat ik er vanuit gaan dat u enigszins bekend bent met lineaire algebra. Dan zult u niet schrikken als ik u vraag naar de *eigenwaarden* van de

volgende 3×3 matrix:

$$A = \begin{bmatrix} 0 & 4 & 2 \\ -1 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}.$$

Dat is een vraagstuk dat equivalent is met de vraag om de nulpunten te berekenen van een derdegraadspolynoom, het *karakteristieke polynoom* van de matrix A. Het zal uw eer te na zijn om hiervoor een electronisch rekentuig in te zetten, maar bedenk dat de wereld vol zit met mensen die geen wiskundige zijn! Deze mensen zullen snel geneigd zijn om gespecialiseerde software in te zetten, en ook om genoegen te nemen met een benadering van de exacte eigenwaarden in de vorm van een eindige decimale ontwikkeling. Eén van de bekendste en kwalitatief beste softwarepaketten voor problemen uit de lineaire algebra is *Matlab*, ontwikkeld door Cleve Moler en Jack Little in de zeventiger jaren, en inmiddels uitgegroeid tot een zowel binnen de academia als in het bedrijfsleven zeer veel gebruikte programmeeromgeving. Dit is wat Matlab als antwoord geeft op mijn vraag om de eigenwaarden van A te berekenen:

```
>> eig(A)

ans =

  1.0e-004 *

  -0.0521 + 0.0902i
  -0.0521 - 0.0902i
   0.1041
```

Hier staat dat `ans`, het antwoord (*answer*) van de door mij gevraagde berekening gelijk is aan het drietal getallen

$$(-5.21 + 9.02i) \times 10^{-6}, \quad (-5.21 - 9.02i) \times 10^{-6}, \quad \text{en} \quad 1.041 \times 10^{-5}.$$

De ongeïnformeerde gebruiker zal hierbij zijn schouders ophalen (of dat nog niet eens) en de geproduceerde antwoorden kritiekloos, of met in het achterhoofd toch de wetenschap dat Matlab net als legio andere softwarepakketten *in zestien decimalen nauwkeurig rekent*, ter kennisgeving aannemen: twee complex geconjugeerde nulpunten, en een derde nulpunt dat reëel is. Niets aan de hand. Matlab is immers in staat om de honderd eigenwaarden van een 100×100 matrix in ongeveer een honderdste van een seconde uit te rekenen op een standaard laptop, dus waarom zouden we argwanend staat tegenover die van een simpele 3×3 matrix?

Ik ga ervanuit dat de wiskundige in u er inmiddels achter is, dat de matrix A de eigenschap heeft, dat A^3 gelijk is aan de *nulmatrix*. Of, dat het eerder genoemde karakteristieke polynoom van A, waarvan de eigenwaarden de nulpunten zijn, het polynoom $p_A(x) = x^3$ is. En dus, dat alledrie de eigenwaarden van A gelijk zijn aan nul. Natuurlijk kunt u op uw beurt, net als de gebruiker, uw schouders ophalen en mompelen dat de wiskunde uiteraard superieur is over het rekentuig, maar eigenlijk hoop ik op de open blik waar ik het eerder over had:

Hoe is het in vredesnaam mogelijk, dat een wereldwijd door miljoenen mensen gebruikt softwarepakket, ontwikkeld door een bedrijf dat nota bene de top-specialisten in dienst heeft op het gebied van de numerieke lineaire algebra, een antwoord produceert van een berekening die iedere eerstejaars wiskundestudent met pen en papier in een paar minuten foutloos kan oplossen, dat reeds in de vijfde (!) decimaal incorrect is?

Bedenk wel, de opmerking dat Matlab in zestien decimalen nauwkeurig rekent is grofweg gesproken correct! U zult waarschijnlijk (hopelijk) niet schrikken van het resultaat van de volgende Matlab-berekening:

```
>> sin(pi)

ans =
    1.224646799147353e-016
```

omdat u zich zal realiseren dat een *numeriek pakket* als Matlab het zich niet kan permitteren om berekeningen *symbolisch* te doen. Het getal π zal daarom *slechts* in zestien decimalen nauwkeurig zijn, en de sinus van dat getal zal dan ook geen nul opleveren. Maar wat er wel uitkomt lijkt gelukkig wel optimale precisie te hebben: de *fout* zit in de zestiende decimaal.

De relatieve precisie van zestien decimalen, ondanks dat we niet gedefinieerd hebben wat we daarmee bedoelen, is mooi verwoord door Lloyd N. Trefethen (Oxford) die aangaf, dat het de afstand tussen twee moleculen in de lucht is in relatie tot de omtrek van de aarde. In dat licht bezien is een fout in de vijfde decimaal natuurlijk volledig onacceptabel!

6.3 De aard van het beestje

Fouten maken is niet alleen menselijk, maar bij uitstek ook *computerlijk*. Het is fysiek onmogelijk om een overaftelbaar oneindige verzameling getallen exact te representeren in een apparaat, en daar ook nog eens exacte

berekeningen mee te doen. In die zin kunnen we niet heen om de beperkingen van een computer. Zelfs als we aannemen dat het mogelijk is om een *aftelbaar* oneindige verzameling getallen exact te representeren, stuiten we op problemen. Deze laatste aanname is precies degene die vaak wordt gedaan om het rekenen op de computer te modelleren. In concreto, schrijf F voor de verzameling van $2^{52}+1$ getallen

$$1, \quad 1+1\times 2^{-52}, \quad 1+2\times 2^{-52}, \quad \ldots \quad , \quad 2-1\times 2^{-52}, \quad 2$$

Definieer vervolgens

$$\mathbb{F} = \bigcup_{j=-\infty}^{\infty} \left(-2^j F\right) \cup \{0\} \cup \bigcup_{j=-\infty}^{\infty} \left(2^j F\right).$$

Dan is $\mathbb{F} = 2\mathbb{F}$ een aftelbaar oneindige verzameling getallen, waarvan *in de praktijk* slechts een eindig deel (het deel voor $-N \leq j \leq N$ voor zekere voldoende grote vaste N) daadwerkelijk in de computer exact gerepresenteerd worden. Om het gedrag van berekeningen op de computer te bestuderen, wordt vaak gedaan alsof *alle* getallen in $\mathbb{F}$ exact gerepresenteerd kunnen worden, omdat berekeningen waarvoor N onvoldoende groot is, veel zeldzamer zijn dan berekeningen waarvoor de relatieve afstand tussen twee opeenvolgende getallen van $\mathbb{F}$ onvoldoende klein is.

Om een analyse van de gevolgen van eindige rekenprecisie op abstracte wijze te kunnen analyseren, is één van de grondbeginselen een heus *axioma*. Dit axioma gebruikt de relatieve machineprecisie ε_m als uitgangspunt. Deze ε_m is het kleinste getal met de eigenschap dat

$$\forall x \in \mathbb{R} : \exists x' \in \mathbb{F} : \quad |x - x'| \leq \varepsilon_m |x|.$$

Voor onze keuze van $\mathbb{F}$ is de waarde van ε_m gelijk aan $2^{-53} \approx 1.11 \times 10^{-16}$, de helft van de relatieve afstand tussen twee getallen in $\mathbb{F}$. Echter, andere keuzes van $\mathbb{F}$ zijn mogelijk. Vooral theoretisch is dit van belang, in de zin dat we soms uitspraken willen doen voor een oneindige rij computers waarvan de machineprecisie naar nul convergeert.

Het Fundamentele Axioma van Eindige Precisie Aritmetiek

Voor alle $x, y \in \mathbb{F}$ bestaat er een ε met $|\varepsilon| \leq \varepsilon_m$ zodanig dat

$$x \circledast y = (x * y)(1+\varepsilon)$$

waarbij $* \in \{+, -, \times, /\}$ en waarbij $\circledast$ de overeenkomstige bewerking op de computer is.

Hiermee wordt bedoeld, dat het door de computer berekende resultaat $1 \oslash 3$ (dat per definitie in $\mathbb{F}$ ligt) van de berekening $1/3$ (van de getallen $1, 3 \in \mathbb{F}$) in relatieve zin een fout in zich draagt van hooguit ε_m. Merk op dat in bovenstaand model $1/3 \notin \mathbb{F}$ en dat het foutief berekenen van $1/3$ dus onvermijdelijk is. Samengevat zal een computer die voldoet aan het axioma de nauwkeurigst mogelijke antwoorden produceren van de elementaire rekenkundige bewerkingen toegepast op twee *machinegetallen*, zoals de getallen uit $\mathbb{F}$ heten.

6.4 Correcte antwoord op de verkeerde vraag

Een belangrijke eigenschap van het rekenen op de computer, die een direct gevolg is van het fundamentele axioma van de eindige precisie aritmetiek, is de volgende. Stel, we hebben twee getallen $x, y \in \mathbb{R}$, niet noodzakelijkerwijs uit $\mathbb{F}$, en we willen $x * y$ berekenen met behulp van de computer. Hierbij is weer $* \in \{+, -, \times, /\}$ één van de vier elementaire rekenkundige bewerkingen. Als inderdaad $x, y \notin \mathbb{F}$ zullen we deze getallen eerst zo goed mogelijk moeten *representeren* in $\mathbb{F}$. Hiervoor introduceren we de functie

$$\mathrm{fl} : \mathbb{R} \to \mathbb{F} : \quad x \mapsto \mathrm{fl}(x)$$

die aan $x \in \mathbb{R}$ een getal $\mathbb{F}$ toevoegt dat daar het dichtst mogelijk bij ligt. Merk op dat hier soms een keuzemogelijkheid is en geloof het of niet, dat er serieuze onderzoekingen zijn gedaan naar de gevolgen van alleen al deze keuze! Hoe dan ook, voorzien van fl beweren we nu:

Voor ieder paar $x, y \in \mathbb{R}$ bestaan er $x', y' \in \mathbb{R}$ zodanig dat

$$\mathrm{fl}(x) \circledast fl(y) = x' * y' \quad \text{en} \quad |x - x'| \leq g(\varepsilon_m)|x|, \quad |y - y'| \leq g(\varepsilon_m)|y|,$$

en waarbij g een functie is met de eigenschap dat $\lim_{x \downarrow 0} g(x) = 0$.

De bewering is dus, dat ondanks dat het berekende resultaat $\mathrm{fl}(x) \circledast fl(y)$ in het algemeen niet exact gelijk is aan het gewenste $x * y$, er getallen x' en y' bestaan waarvoor $\mathrm{fl}(x) \circledast fl(y)$ wel exact gelijk is aan $x' * y'$, en waarvoor bovendien geldt dat deze twee getallen in de orde van de machineprecisie afliggen van de getallen waarop we de berekening hadden willen uitvoeren.

En weer kunnen we onze schouders ophalen: de computer verschaft ons het *exacte* antwoord van een berekening *waarom we niet hebben gevraagd*. Wat is het nut van deze observatie?

Conceptueel is het nut als volgt. Er bestaan legio wiskundige berekeningen waarbij het zo is dat als we deze toepassen op zeer licht gewijzigde

getallen, het resultaat compleet anders wordt, zelfs als iedere berekening zonder fouten zou worden gedaan. Dit is dan dus blijkbaar een *wiskundige* eigenschap, inherent aan het type van de berekening. Maar het gevolg is, dat zelfs als we kunnen aantonen dat de op een computer uitgevoerde berekeningen het *exacte* antwoord geeft op hetzelfde probleem met licht gewijzigde getallen, we redelijkerwijs *nooit mogen verwachten* dat de computer een nauwkeurig antwoord geeft. In dat geval geldt dus:

don't blame the computer, blame the maths!

Is het probleem daarentegen zo, dat indien toegepast op nabij gelegen getallen, het resultaat ook niet al te veel verandert (als het probleem *differentieerbaar* is in zijn inputs) dan zal een algoritme dat het juiste antwoord produceert op een nabijgelegen probleem, binnen de grenzen van wat mogelijk is een nauwkeurig antwoord geven. Kortom, het krijgen van een exact antwoord op een licht gewijzigd probleem is in feite het beste wat je van een algoritme kunt verwachten, en of dit leidt tot een nauwkeurig uitgevoerde berekening op een computer hangt, in dat geval, af van het probleem.

6.5 Een afschrikwekkende matrix

Laten we, gewapend met onze nieuw verworven kennis, terugkeren naar ons eerdere voorbeeld, met de 3×3 matrix A waarvan Matlab niet in staat bleek nauwkeurige eigenwaarden te berekenen, ondanks dat deze nota bene alledrie gelijk waren aan nul. Zoals we al meldden, zijn de eigenwaarden van A de nulpunten van het karakteristieke polynoom $p_A(x) = x^3$. Veronderstel nu dat we de getallen in A een heel klein beetje veranderen. Dan veranderen ook de coëfficiënten van het karakteristieke polynoom. Stel dat het resultaat het heel onschuldig ogende polynoom

$$p_{\tilde{A}}(x) = x^3 + \varepsilon$$

is voor een klein getalletje ε. Dan zijn de exacte nulpunten van dit getal gelijk aan de drie derdemachtswortels van ε in het complexe vlak, waarvan er één reëel is. Merk tevens op dat

$$\sqrt[3]{|\varepsilon|} \approx 4.8 \times 10^{-6}.$$

Dus, bij een *minimale verstoring* van de matrix A zal zelfs een algoritme dat de exacte eigenwaarden oplevert van een naburige matrix, een enorm

verlies van nauwkeurigheid te zien geven. Maar ligt dat dan aan het algoritme? Nee, het ligt aan de wiskundige eigenschappen van nulpunten van polynomen, en aan het simpele gegeven dat een computer noodzakelijkerwijs met eindige precisie rekent. In het bijzonder ligt de "schuld" dus niet bij Matlab!

6.6 Gewiekstheid gewenst en geboden

Kent u het Gram-Schmidt proces nog? Dat was een algoritme om bijvoorbeeld drie gegeven (lineair onafhankelijke) vectoren a_1, a_2, a_3 in $\mathbb{R}^3$ te orthonormaliseren, oftewel, loodrecht op elkaar te zetten. De diverse stappen laten zich als volgt algoritmisch omschrijven:

- schaal a_1 op lengte één, en noem het resultaat q_1;
- bereken de loodrechte projectie van a_2 op q_1;
- trek deze af van a_2;
- schaal het resultaat op lengte één, en noem het resultaat q_2;
- de vectoren q_1 en q_2 zijn nu orthonormaal;
- projecteer a_3 op het vlak opgespannen door q_1 en q_2;
- trek het resultaat af van a_3;
- schaal het resultaat op lengte één, en noem het resultaat q_3;
- de vectoren q_1, q_2 en q_3 zijn nu orthonormaal.

Als u deze stappen met pen en papier exact uitvoert, dan resulteert een waarlijk orthonormale basis; a_1 is hierbij een veelvoud van q_1, a_2 is een lineaire combinatie van q_1 en q_2, en a_3 is (natuurlijk) een lineaire combinatie van q_1, q_2 en q_3, oftewel,

$$r_{11}q_1 = a_1, \quad r_{12}q_1 + r_{22}q_2 = a_2 \quad r_{13}q_1 + r_{23}q_2 + r_{33}q_3 = a_3$$

voor zekere reële getallen $r_{11}, r_{12}, r_{22}, r_{13}, r_{23}$ en r_{33}. In matrix-termen:

$$\left[\begin{array}{c|c|c} a_1 & a_2 & a_3 \end{array}\right] = \left[\begin{array}{c|c|c} q_1 & q_2 & q_3 \end{array}\right] \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ 0 & r_{22} & r_{23} \\ 0 & 0 & r_{33} \end{bmatrix}.$$

We hebben een zogenaamde QR-decompositie berekend van de matrix A die kolommen a_1, a_2, a_3 heeft: Q heeft onderling orthonormale kolommen

q_1, q_2, q_3, en R is een *bovendriehoeksmatrix*, en

$$A = QR.$$

In het algemeen, en in de *wiskundige zin*, zal de orthonormale basis q_1, q_2, q_3 nauwelijks veranderen als a_1, a_2, a_3 licht worden verstoord, alhoewel dit soms wel zo is: bijvoorbeeld als a_3 een heel klein beetje boven het a_1, a_2 vlak ligt, en er na de verstoring ineens net onder ligt.

Echter, hoe wereldberoemd het Gram-Schmidt algoritme ook is, de bedenkers ervan hadden niet kunnen vermoeden dat als het wordt uitgevoerd op een computer die voldoet aan het fundamentele axioma van de eindige precisie aritmetiek, het *niet* resulteert in een (vrijwel) orthonormale basis van een *naburig gelegen* stel vectoren a_1', a_2', a_3'. Dat is dus een tekortkoming van het *algoritme*, en niet van de *wiskunde*! Om dit in te zien geven we eerst de formules voor q_1, q_2, q_3 in termen van a_1, a_2, a_3 als volgt,

$$q_1 = \frac{a_1}{\|a_1\|}$$

en vervolgens

$$q_2 = \frac{\hat{q}_2}{\|\hat{q}_2\|}, \quad \text{waarbij} \quad \hat{q}_2 = a_2 - q_1 q_1^\top a_2$$

en tot slot

$$q_3 = \frac{\hat{q}_3}{\|\hat{q}_3\|}, \quad \text{waarbij} \quad \hat{q}_3 = a_3 - q_1 q_1^\top a_3 - q_2 q_2^\top a_3.$$

Hierbij is $v^\top$ de *gespiegelde* van de vector v, en dus is $v^\top w$ het *inproduct* tussen v en w, en is $\|v\|$ de lengte van v. We illustreren deze berekeningen met een expliciet rekenvoorbeeld.

Voorbeeld. Laat $\varepsilon \in \mathbb{F}$ een getalletje zijn met de eigenschap dat $\mathrm{fl}(1 + 2\varepsilon^2) = 1$, en pas het Gram-Schmidt algoritme toe op de vectoren

$$a_1 = \begin{bmatrix} 1 \\ \varepsilon \\ \varepsilon \end{bmatrix}, \quad a_2 = \begin{bmatrix} 1 \\ \varepsilon \\ 0 \end{bmatrix}, \quad a_1 = \begin{bmatrix} 1 \\ 0 \\ \varepsilon \end{bmatrix}$$

Dan:

$$\|a_1\| = \sqrt{1 + \varepsilon^2 + \varepsilon^2} \sim 1,$$

en dus $q_1 = a_1$. Om q_2 te bepalen berekenen we het inproduct

$$q_1^\top a_2 = 1 + \varepsilon^2 \sim 1,$$

en dus,

$$\hat{q}_2 = a_2 - 1 \cdot q_1 = \begin{bmatrix} 0 \\ 0 \\ -\varepsilon \end{bmatrix}.$$

Schaling op lengte één gaat exact wegens $\varepsilon \in \mathbb{F}$:

$$q_2 = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}.$$

We trekken nu eerst $q_1 q_1^\top a_3$ af van a_3 en noemen het resultaat $\hat{\hat{q}}_3$:

$$\hat{\hat{q}}_3 = \begin{bmatrix} 1 \\ 0 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 1 \\ \varepsilon \\ \varepsilon \end{bmatrix} [1\ \varepsilon\ \varepsilon] \begin{bmatrix} 1 \\ 0 \\ \varepsilon \end{bmatrix} \sim \begin{bmatrix} 1 \\ 0 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 1 \\ \varepsilon \\ \varepsilon \end{bmatrix} = \begin{bmatrix} 0 \\ -\varepsilon \\ 0 \end{bmatrix},$$

en vervolgens trekken we $q_2 q_2^\top a_3$ af van $\hat{\hat{q}}_3$,

$$\hat{q}_3 = \begin{bmatrix} 0 \\ -\varepsilon \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} [0\ 0\ -1] \begin{bmatrix} 1 \\ 0 \\ \varepsilon \end{bmatrix} \sim \begin{bmatrix} 0 \\ -\varepsilon \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ \varepsilon \end{bmatrix} = \begin{bmatrix} 0 \\ -\varepsilon \\ -\varepsilon \end{bmatrix},$$

waarna schaling op lengte één geeft dat

$$q_3 = \begin{bmatrix} 0 \\ -\mathrm{fl}(\frac{1}{2}\sqrt{2}) \\ -\mathrm{fl}(\frac{1}{2}\sqrt{2}) \end{bmatrix}.$$

Dus, de orthonormale basis berekend op een computer met het Gram-Schmidt algoritme bestaat uit de vectoren

$$q_1 = \begin{bmatrix} 1 \\ \varepsilon \\ \varepsilon \end{bmatrix}, \quad q_2 = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} \quad \text{and} \quad q_3 = \begin{bmatrix} 0 \\ -\mathrm{fl}(\frac{1}{2}\sqrt{2}) \\ -\mathrm{fl}(\frac{1}{2}\sqrt{2}) \end{bmatrix},$$

waarvan de laatste een hoek maakt van 45° met de tweede. Dat is nauwelijks recht te noemen!

Dit is natuurlijk een kunstmatig gefabriceerd voorbeeld, maar het is een feit dat het toepassen van Gram-Schmidt op tientallen of honderden vectoren van grote lengte resulteert in bases die verre van orthonormaal zijn, doordat de kleine ongewilde effecten *accumuleren*.

Numerieke lineaire algebra heeft echter een simpele oplossing aangedragen om bovenstaand probleem te verhelpen, door in te zien dat het probleem

wordt veroorzaakt door de projectie van a_3 op het vlak opgespannen door q_1 en q_2 te berekenen als

$$q_3 = \frac{\hat{q}_3}{\|\hat{q}_3\|}, \quad \text{waarbij} \quad \hat{q}_3 = a_3 - q_1 q_1^\top a_3 - q_2 q_2^\top a_3.$$

Deze formule is namelijk alleen correct indien q_1 en q_2 *daadwerkelijk orthonormaal* zijn (en hetzelfde geldt uiteraard voor verdere vectoren $q_4, q_5, \ldots$ die op soortgelijke wijze worden berekend. Dus, rekenfouten in $q_1, \ldots, q_k$ werken ook door in q_{k+1} doordat de formule waarmee q_{k+1} wordt uitgerekend, niet meer correct is, los van het feit dat in de evaluatie van de formule ook nog fouten worden gemaakt. Ondanks dat het eerste probleem kan worden verholpen door een formule te gebruiken die ook correct is als de vectoren $q_1, \ldots, q_k$ niet meet precies orthonormaal zijn, is dat niet nodig. Gelukkig maar, want dergelijke formules kosten weer erg veel rekenwerken tijd. Het blijkt voldoende om de berekening van bijvoorbeeld q_3 licht aan te passen tot

$$q_3 = \frac{\hat{q}_3}{\|\hat{q}_3\|}, \quad \text{waarbij} \quad \hat{q}_3 = \hat{\hat{q}}_3 - q_2 q_2^\top \hat{\hat{q}}_3, \quad \hat{\hat{q}}_3 = a_3 - q_1 q_1^\top a_3.$$

Het enige verschil zit er dus in, dat hierin de term $q_2 q_2^\top \hat{\hat{q}}_3$ wordt uitgerekend, tegen $q_2 q_2^\top a_3$ in de eerdere methode. Echter, omdat $q_2 q_2^\top \hat{\hat{q}}_3 = q_2 q_2^\top (a_3 - q_1 q_1^\top a_3) = q_2 q_2^\top a_3$ maakt dit *in theorie* geen verschil, immers, $q_2^\top q_1 = 0$. Voor deze variant kan echter bewezen worden dat hij veel beter eigenschappen heeft in eindige precisie aritmetiek.

Voorbeeld. We illustreren deze laatste opmerking door bovenstaand voorbeeld te vervolgen, en berekenen q_3 nu op de alternatieve wijze als

$$\hat{\hat{q}}_3 = \begin{bmatrix} 0 \\ -\varepsilon \\ 0 \end{bmatrix},$$

gevolgd door de gewijzigde stap,

$$\hat{q}_3 = \begin{bmatrix} 0 \\ -\varepsilon \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} [0 \; 0 \; -1] \begin{bmatrix} 0 \\ -\varepsilon \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ -\varepsilon \\ 0 \end{bmatrix},$$

die na schaling resulteert in

$$q_3 = \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix}.$$

De drie vectoren berekend met dit gemodificeerde Gram-Schmidt algoritme zijn derhalve

$$q_1 = \begin{bmatrix} 1 \\ \varepsilon \\ \varepsilon \end{bmatrix}, \quad q_2 = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} \quad \text{and} \quad q_3 = \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix}.$$

Ondanks dat deze vectoren ook niet precies orthonormaal zijn, zijn ze een stuk orthonormaler dan de met het standaard Gram-Schmidt algoritme berekende vectoren.

6.7 Het QR-algoritme

Het leek er misschien even op dat ik afdwaalde, door u met het Gram-Schmidt proces en zijn tekortkomingen te vermoeien, daar waar we het eerst over eigenwaarden van matrices hadden. Echter, om af te ronden wil ik beide concepten met elkaar combineren. De vraag is namelijk: hoe is Matlab in staat om eigenwaarden van een (grote) matrix A te berekenen, en te garanderen dat de berekende getallen de eigenwaarden zijn van een nabijgelegen matrix?

Het blijkt zo te zijn dat algoritmes die gebaseerd zijn op het vinden van nulpunten van het karakteristieke polynoom niet de gewenste eigenschappen hebben. Wat verbazend genoeg wel werkt, is het volgende algoritme, dat niet alleen de juiste eigenschappen heeft, maar (in iets geavanceerdere vorm) ook nog eens razendsnel convergeert.

QR-algoritme (eenvoudige vorm)

Gegeven een matrix A_0, laat $j = 0$ en itereer

- Bereken de QR-decompositie $A_j = QR$ van A_j;
- Laat $A_{j+1} = RQ$.

Het berekenen van de QR-decompositie van A_j moet dan *wel* gebeuren met het gemodificeerde Gram-Schmidt algoritme uit de voorgaande sectie, of liever nog met de nog betere variant bedacht door Aliston Householder. Er blijkt dat dan, onder milde voorwaarden, de rij van matrices A_j convergeert naar een diagonaalmatrix (als $A = A^\top$) of een bovendriehoeksmatrix in het algemene geval. In beide gevallen zijn de diagonaal-elementen de (benaderingen van) de eigenwaarden van de start-matrix A_0, en dus van de nulpunten van het corresponderende karakteristieke polynoom.

Merk op dat de berekeningen in het AR-algoritme conceptueel bijzonder

eenvoudig zijn, en in die zin is het algoritme bijna *triviaal*. Echter, om volledig te doorgronden wanneer en waarom het werkt, kan een levenslang onderzoek nog steeds onvoldoende zijn: de Amerikaanse wiskundige David Watkins *begreep* het QR-algoritme reeds in 1982, volgens de title van zijn artikel [4] voor *SIAM Review*, maar in een dozijn verdere artikelen over hetzelfde onderwerp komt hij steeds weer tot nieuwe inzichten. In 2008 schreef hij opnieuw een artikel [5] voor hetzelfde tijdschrijft *SIAM Review*, om zich daarin af te vragen of hij er al niet genoeg over had geschreven, en die vraag vervolgens negatief te beantwoorden. De *methode* laat zich prima introduceren in een Bachelorvak over numerieke lineaire algebra, en zo ook een deel van de analyse (vooral die voor reëel symmetrische matrices) maar de algemene theorie is buitengewoon complex!

Referentie [1] is een prima introducerende tekst voor numerieke lineaire algebra en de concepten *conditionering* en *stabiliteit*. Het boek [3] is een zeer compleet naslagwerk met de eigenschappen van veel standaard-algoritmes in eindige precisie aritmetiek; tot slot ligt [2] in het midden tussen de eerstgenoemde twee boeken.

Bibliografie

[1] L.N. Trefethen en D. Bau III (1997). *Numerical Linear Algebra*. SIAM, Society for Industrial and Applied Mathematics, Philadelphia.

[2] G.H. Golub en C.F. Van Loan (2013). *Matrix Computations*. Fourth edition. The John Hopkins University Press.

[3] N.J. Higham (1996). *Accuracy and Stability of Numerical Algorithms*. SIAM, Society for Industrial and Applied Mathematics, Philadelphia.

[4] D.S. Watkins (1982). Understanding the QR-algorithm, SIAM Review, Vol.24, pp. 427-440.

[5] D.S. Watkins (2008). The QR-algorithm revisited. SIAM Review, Vol.50, pp. 133–145.

7 Praktikum
Benne de Weger

7.1 Hoe snel kun je vermenigvuldigen?

De eerste vraag is: wat bedoel je met snel? Rekenen met een stuk papier en een pen gaat al gauw sneller dan uit het hoofd; met een zakjapanner gaat het sneller dan op papier; tegen een computer kan geen mens op en die computer waar je 10 jaar geleden zo enthousiast over was vind je nu tergend sloom: zelfs je mobiel doet het nu nog beter.

Dat bedoelen we dus niet met snelheid. We willen snelheid onafhankelijk van hulpmiddelen kunnen uitdrukken: het gaat erom hoe goed je methode (of: algoritme) is. Dat noemen we: complexiteit van algoritmen.

Op school begon het leren vermenigvuldigen met herhaald optellen. Maar het wordt je al gauw afgeleerd om het zo te blijven doen. Waarom? Omdat de methode van herhaald optellen slechte complexiteit heeft, en er een, ook makkelijke, methode bestaat met veel betere complexiteit: de "basisschoolmethode", je kent hem nog wel.

```
  74
  23
---- x
 222
148
---- +
1702
```

We zullen in dit praktikum zien dat optellen lineaire complexiteit heeft, vermenigvuldigen door herhaald optellen exponentiële complexiteit, en de "basisschoolmethode" kwadratische complexiteit. Nu is het zo dat vrijwel alle mensen daar blijven steken, voor de rest van hun leven. Maar wij vanaf vandaag niet meer. We gaan ontdekken dat vermenigvuldigen echt sneller kan dan kwadratisch. Dit verrassende feit, dat tot mijn verbazing onder wiskundigen niet goed bekend is, is ontdekt in 1960 door Anatolii Karatsuba (uit Rusland).

Ook over zoiets triviaals als vermenigvuldigen valt dus nog iets te leren!

Als er tijd over is kunnen we nog iets doen aan de complexiteit van machtsverheffen (maar dan wel in het kader van modulo-rekenen). Dat snellere vermenigvuldigen blijkt dan ook nog nuttig te zijn in cryptografische toepassingen. Het zou zomaar in je bankpasje kunnen zitten.

7.2 Elementair is niet hetzelfde als triviaal

Sommige wiskundigen denken dat, dat elementair en triviaal hetzelfde is (zie het "Ten geleide" van Jan Wiegerinck[1] in dit boekje). Ik vind van niet. Een redenering die volslagen elementair is kan razend ingewikkeld zijn, en heel lastig om op te komen; maar als je eenmaal ziet hoe het moet, kan het stap voor stap goed te volgen zijn, en blijkt er niets moeilijks of abstracts te gebeuren. Als voorbeelden daarvan gaan we in dit praktikum een paar Diophantische vergelijkingen oplossen; dat zijn vergelijkingen waarbij we uitsluitend gehele getallen als oplossingen toestaan. Vaak zien die problemen er triviaal uit. Soms zijn ze dat ook: de vraag welke machten van 2 en 3 precies 1 verschillen is vrijwel triviaal op te lossen.

Een beroemde Diophantische vergelijking is die van Ramanujan-Nagell: kan een kwadraat vermeerderd met 7 precies een macht van 2 opleveren? Ja, dat kan: $181^2 = 32761$, en $32768 = 2^{15}$. En er zijn nog een paar kleinere oplossingen, die je zo kunt vinden. Maar er is een grotere? Srinavasa Ramanujan (uit India) vermoedde in 1915 van niet, en Trygve Nagell (uit Noorwegen) bewees dat voor het eerst, in 1948. Geen elementair bewijs, laat staan triviaal. Sindsdien zijn er vele andere bewijzen van gegeven, maar bij de meeste daarvan heb je nog op z'n minst een stukje serieuze algebraïsche getaltheorie nodig, en dat noem ik niet meer "elementair".

Maurice Mignotte (uit Frankrijk) vond in 1984 een echt elementair bewijs. "Elementair" betekent hier dan zoiets als: er wordt geen theorie gebruikt die verder gaat dan modulo-rekenen, en je moet weten waarom $\sqrt{2}$ irrationaal is. Een eerstejaarsstudent kan het begrijpen, en ik denk dat je het bij Wiskunde D ook wel moet kunnen doen. Maar triviaal is het zeker niet: het bewijs zit ingenieus in elkaar, en er gebeurt ook nog wel een wondertje.

We beginnen met een vergelijking van hetzelfde type: $x^2 + 2 = 3^n$, waarbij de door Mignotte gebruikte technieken een stuk eenvoudiger uitpakken. En dan kijken we hoever we met het oplossen van $x^2 + 7 = 2^n$ komen. In de elektronische versie van dit boekje, die na afloop van de cursus op de PWN-website gepubliceerd wordt, zal ik de oplossing helemaal uitschrijven.

[1] Overigens geeft het Van Dale Etymologisch Woordenboek (van Veen en van der Sijs, 1997) ook een interessante verklaring voor de afkomst van het woord triviaal: "*triviaal* [onbeduidend] {1553} < frans *trivial* [idem] < latijn *trivialis* [algemeen toegankelijk, alledaags], van *trivium* [wegsplitsing, driesprong, de straat] (*innati triviis* [zij die opgegroeid zijn op de straat, het straatpubliek]), van *tri-* [drie-] + *via* [weg].".

Voor wie is PWN interessant?

Beroepswiskundigen
Wiskundeleraren
Bedrijven
Leerlingen en studenten
Breed publiek

Platform Wiskunde Nederland is hét landelijke loket voor alles wat met wiskunde te maken heeft.

PWN behartigt de belangen van, en fungeert als spreekbuis voor, de gehele Nederlandse wiskunde.

Platform Wiskunde Nederland | Science Park 123 | kamer L013 | 1098 XG Amsterdam | 020 592 40 06

Ga voor meer informatie naar:
www.platformwiskunde.nl

platform
wiskunde nederland