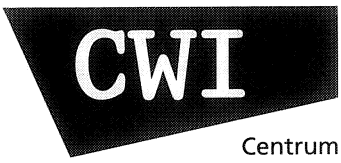


Centrum Wiskunde & Informatica

Wiskunde: de uitdaging

Vakantiecursus 2010

27 en 28 augustus 2010 in Amsterdam
3 en 4 september 2010 in Eindhoven

CWI syllabus 60

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

Deze cursus is mede mogelijk gemaakt door een subsidie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek.

ISBN: 978 90 6196 557 2
NUR-Code: 918

Inhoud

Docenten

Prof. dr. J.J.O.O. Wiegerinck
Korteweg-de Vries Instituut voor Wiskunde, Universiteit van Amsterdam
Postbus 94248, 1090 GE Amsterdam
J.J.O.O.Wiegerinck@uva.nl

Prof. dr. F. Beukers
Universiteit Utrecht, Faculteit Bètawetenschappen, Departement Wiskunde
Budapestlaan 6, 3584 CD Utrecht
F.Beukers@uu.nl

Prof. dr. ir. J.E. Frank
Centrum Wiskunde & Informatica, Dynamical Systems and Numerical Analysis (MAC1) Postbus 94079, 1090 GB Amsterdam
J.E.Frank@cwi.nl

Dr. G.W.Q. Puite
Technische Universiteit Eindhoven, Faculteit Wiskunde en Informatica
Postbus 513, 5600 MB Eindhoven
G.W.Q.Puite@tue.nl

Prof. dr. A.C.M. van Rooij (emeritus)
Radboud Universiteit Nijmegen, Faculteit FNWI, secretariaat Wiskunde
Postbus 9010, 6500 GL Nijmegen
W.vandeSluis@math.ru.nl

Dr. V. Rottschäfer
Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden
vivi@math.leidenuniv.nl

Prof. dr. M.J. Sjerps
Nederlands Forensische Instituut (NFI). Korteweg-de Vries Instituut voor Wiskunde, Universiteit van Amsterdam, Postbus 94248, 1090 GE Amsterdam
m.sjerps@nfi.minjus.nl

Dr. ir. I. Smeets
Liacs, Universiteit Leiden, Postbus 9512, 2300 RA Leiden
ionica.smeets@gmail.com

Dr. B. de Weger
Technische Universiteit Eindhoven, Faculteit Wiskunde en Informatica
Cryptologie, Coding, Crypto-groep, Postbus 513, 5600 MB Eindhoven
b.m.m.d.weger@tue.nl

Leden Programmacommissie Vakantiecursus

Marian Kollenveld (voorzitter)
Leeuwendaallaan 43, 2281 GK Rijswijk
voorzitter@nvvw.nl

Bram van Asch
Technische Universiteit Eindhoven, Postbus 513, 5600 MB Eindhoven
a.g.v.asch@tue.nl

Frits Beukers
Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht
F.Beukers@uu.nl

Jan van de Craats
Korteweg-de Vries Instituut voor Wiskunde, Universiteit van Amsterdam,
FNWI, Postbus 94248, 1090 GE Amsterdam
J.vandeCraats@uva.nl

Jan van Maanen
Freudenthal Instituut, Aidadreef 12, 3561 GE Utrecht
maanen@fi.uu.nl

Kees Oosterlee
Centrum Wiskunde & Informatica, Postbus 94079, 1090 GB Amsterdam
C.W.Oosterlee@cwi.nl

Ionica Smeets
LIACS, Mathematisch Instituut, Universiteit Leiden
Postbus 9512, 2300 RA Leiden
ionica.smeets@gmail.com

Jeroen Spandaw
Technische Universiteit Delft, EWI, Mekelweg 4, 2628 CD Delft
J.G.Spandaw@tudelft.nl

Ruud Stolwijk
Cito, Nieuwe Oeverstraat 50, 6801 MG Arnhem
Ruud.Stolwijk@cito.nl

Marco Swaen
Korteweg-de Vries Instituut voor Wiskunde, Universiteit van Amsterdam
Postbus 94248, 1090 GE Amsterdam
m.d.g.swaen@uva.nl

Jan Wiegerinck
Korteweg-de Vries Instituut voor Wiskunde, Universiteit van Amsterdam
Postbus 94248, 1090 GE Amsterdam
J.J.O.O.Wiegerinck@uva.nl

Wiskunde: de uitdaging

Jan Wiegerinck
Korteweg-de Vries Instituut voor Wiskunde
Universiteit van Amsterdam
e-mail: J.J.O.O.Wiegerinck@uva.nl

Deze 64-ste vakantiecursus wordt niet meer onder de inspirerende leiding van Jan Aarts georganiseerd, ik heb het stokje van Jan mogen overnemen. Jan heeft dit werk vele jaren gedaan, en gezien het succes van de cursussen, heeft hij het heel goed gedaan! Voor mij zal de uitdaging zijn om het niveau van Jan te handhaven. Mede namens de vele cursisten die van de vakantiecursussen genoten hebben, wil ik Jan van harte voor zijn werk bedanken. Ik hoop dat we hem nog vaak als bezoeker van de cursus zullen tegenkomen!

De wiskunde kent vele uitdagingen. Allereerst denk ik dan aan de wiskundige problemen waar je mee kunt worstelen. Soms zijn ze frustrerend, meestal is het leuk om er over na te denken, en het geeft een enorme kick als je echt iets gevonden hebt. Een uitdaging met onmiddellijke consequenties is het wiskunde onderwijs. Hoe breng ik de wiskunde over, hoe maak ik de studenten enthousiast en hoe zorg ik ervoor dat ik door de stof heen kom. Dat is al een uitdaging binnen de wiskundeopleiding aan de universiteit waar de studenten intrinsiek in wiskunde zijn geïnteresseerd. Hoe moeilijk zal het dan in het middelbaar onderwijs zijn! En dan is er ook de organisatorische uitdaging voor de wiskunde. Organiseer de wiskunde en de wiskundigen in Nederland zó dat het groot publiek, de overheid en het bedrijfsleven het belang van ons vak zien, en onze stem horen. NVvW, KWG en NWO werken hard aan een Platform Wiskunde Nederland dat deze laatste uitdaging aan zal gaan.

Maar in de vakantiecursus is de uitdaging minder zwaar, het thema is geïnspireerd door de komende Internationale Wiskunde Olympiade, die in 2011 in Nederland wordt gehouden. Dat betekent uitdagende opgaven voor onze beste leerlingen, en voor ons de uitdaging om hen goed voor te bereiden!

De voordracht van **Quintijn Puite** sluit direct bij dit thema aan. Hij spreekt over de verrassende wiskunde bij de olympiade en hoe gezond verstand je bij de opgaven kan helpen.

Ionica Smeets snijdt lichtvoetig een teer onderwerp aan met Gênante Vragen. Wiskundige vragen die iedere gek kan stellen, maar geen 1000 wijzen kunnen beantwoorden, zoals het beruchte Collatz probleem. Wel een wiskundige uitdaging natuurlijk!

Maar zogauw je over uitdagingen gaat praten blijkt al snel dat er vele uitdagingen voor de wiskunde bestaan en in de wiskunde aanwezig zijn.

Vivi Rottschäfer zal ons vertellen over de vragen die het bedrijfsleven ieder jaar weer aan de wiskunde stelt en over de Studiegroep Wiskunde met de Industrie, waarin wordt geprobeerd zulke vragen op te lossen.

Over de rol van wiskunde en statistiek in de rechtszaal is de laatste tijd veel te doen geweest. Hoe het met de statistiek in het strafrecht precies in elkaar zit, zal **Marjan Sjerps** ons uitleggen.

De weersvoorspelling interesseert ons allemaal. Hoe moeilijk het is een voorspelling te doen die beter is dan 'het wordt morgen ongeveer als vandaag', en wat de wiskunde daarin betekent, is het onderwerp van **Jason Frank**. **Benne de Weger** pakt het heikele onderwerp van Internet Security bij de kop. Hij spreekt over het RSA cryptografisch systeem, en de kwetsbare kanten daarvan.

Meer zuiver wiskundig, maar niet minder uitdagend zijn de zaken waar **Frits Beukers** en **Arnoud van Rooij** over spreken. Diophantische vergelijkingen (vergelijkingen waarbij men oplossingen in de gehele getallen zoekt) en rijen en reeksen, zijn onderwerpen die de wiskundigen al eeuwen bezig houden en altijd uitdagend blijven.

Bij elkaar een zeer gevarieerd programma met goede sprekers die verstand van zaken hebben. Ik hoop dat u ervan zult genieten!

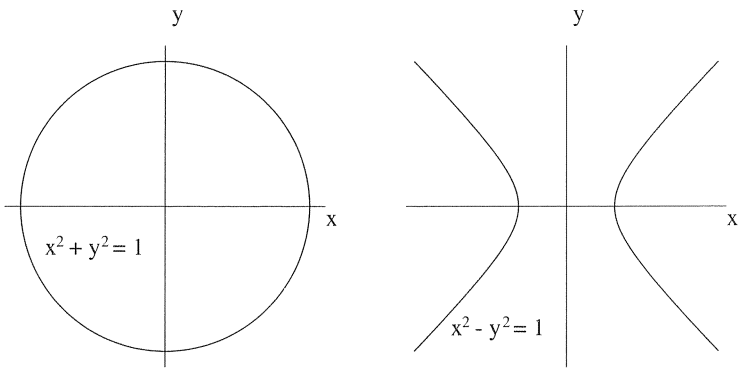
Diophantische vergelijkingen
Een onmogelijke uitdaging

Frits Beukers
Universiteit Utrecht
e-mail: F.Beukers@uu.nl

1 Wat is het probleem?

"Wetende, mijn beste vriend Dionysius, dat jij ernaar verlangt om problemen in de getallen te onderzoeken, heb ik getracht om je, vanuit de grondslagen, het karakter en de kracht die in getallen schuilt uiteen te zetten. Door onbekendheid met het onderwerp zal het eerste begin misschien moeilijk lijken, de beginner kan snel wanhopig worden als succes uitblijft. Maar jij, met je enthousiasme als drijfveer, en mijn begeleiding als leermeester, zult snel in de materie thuisraken. Want passie om te leren, geleid door goede instructie zijn de middelen tot snelle vooruitgang".
Aldus begint, zeer vrij vertaald, de *Arithmetica* van Diophantus van Alexandrië, een boek uit de tijd rond het begin van de jaartelling dat, in tegenstelling tot veel Grieks werk over wiskunde, over getaltheorie gaat. De Arithmetica is een verzameling van 13 boeken, waarvan veel verloren is gegaan. Zes delen, bekend als de Griekse versie, zijn via de Byzantijnse wereld in de 16e eeuw in Europa terecht gekomen en hebben sinds die tijd een inspiratiebron gevormd voor de Europese wiskunde. Vier andere delen zijn in Arabische vertaling rond 1970 ontdekt, hoewel er nog steeds discussie is of het werkelijk om verloren delen van de Arithmetica gaat. In ieder geval staan deze delen bekend als de Arabische versie. In de Arithmetica behandelt Diophantus een lange serie wiskundeproblemen waarin een oplossing in rationale getallen (breuken) gevraagd wordt.
Ter illustratie nemen we een voorbeeld dat bij Diophantus al welbekend was.

Het is algemeen bekend dat de vergelijkingen $x^2 - y^2 = 1$ en $x^2 + y^2 = 1$ de vergelijkingen zijn van een hyperbool en een cirkel.



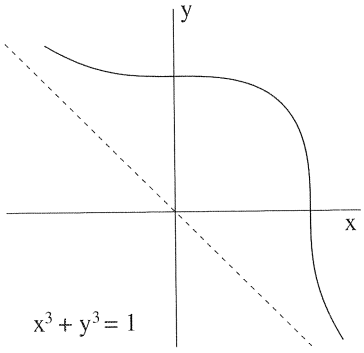
De plaatjes die we hierboven zien zijn een beeld van de oplossingsverzameling van de twee vergelijkingen in de reële getallen x, y. Laten we nu de volgende academische vraag stellen: wat zijn de oplossingen van $x^2 - y^2 = 1$ in rationale getallen (breuken) x, y? En dezelfde vraag voor $x^2 + y^2 = 1$. Anders gezegd, bepaal de punten op bovenstaande hyperbool en cirkel waarvan de coördinaten rationale getallen zijn. Het antwoord op deze vragen was al bij Diophantus, en zelfs lang daarvoor, bekend. In de volgende paragraaf zullen we de oplossing geven.
In elk geval hebben we nu twee voorbeelden van een diophantische vergelijking gezien. In zijn meest algemene vorm, en in moderne taal, kan een diophantische vergelijking als volgt beschreven worden. Kies een veelterm (of polynoom) $F(x_1, \ldots, x_n)$ in n variabelen $x_1, \ldots, x_n$ met gehele getallen als coëfficienten. De vergelijking $F(x_1, \ldots, x_n) = 0$ in de gehele of rationale onbekenden $x_1, \ldots, x_n$ noemen we een *diophantische vergelijking*. De veeltermen uit de eerste twee voorbeelden zijn natuurlijk $F = x^2 - y^2 - 1$ en $F = x^2 + y^2 - 1$. Een van de beroemdste diophantische vergelijkingen die van Pierre de Fermat,

$$x^n + y^n = z^n \quad \text{in } x, y, z \text{ positief geheel.}$$

De exponent n is daarbij een gegeven geheel getal ≥ 2. In de volgende paragraaf zien we dat, als $n = 2$, er oneindig veel oplossingen zijn. Maar Fermat vermoedde al rond 1635 dat deze vergelijking geen oplossing heeft als $n \geq 3$. Gedurende 350 jaar hebben talloze wiskundigen geprobeerd Fermat's vermoeden aan te tonen, maar zonder succes. Wel hebben deze pogingen aanleiding gegeven tot nieuwe ontwikkelingen in de getaltheorie. Pas in 1994 slaagde Andrew Wiles erin het vermoeden van Fermat te bewijzen. Wiles deed nog veel meer, hij gaf namelijk een bewijs van het zogenaamde Shimura-Taniyama-Weil vermoeden en Fermat was hiervan een gevolg. Het bedwingen van Fermat's probleem was een dermate grote triomf van het menselijk vernuft, dat het voorpagina nieuws was voor bijvoorbeeld de *New York Times*, en zijn er postzegels uitgebracht om Fermat en zijn vergelijking te herdenken.

Ook zijn er diverse boeken over Wiles' vondst geschreven, met bijbehorende historie, waarvan ik S. Sing, *Fermat's Last Theorem* in het bijzonder kan aanraden. Een andere aanrader is A.J. van der Poorten, *Notes on Fermat's Last Theorem* maar deze vereist een flinke portie wiskundige achtergrond.

Stand van zaken Neem nu het geval $n = 3$ van Fermat's vergelijking, dus $x^3 + y^3 = z^3$, en deel door z^3. We krijgen $(x/z)^3 + (y/z)^3 = 1$. Na vervanging van de breuken $x/z, y/z$ door de letters x, y zien we dat volgens Fermat de kromme $x^3 + y^3 = 1$ geen rationale punten bevat behalve de voor de hand liggende $(0, 1)$ en $(1, 0)$. Hier is een plaatje van $x^3 + y^3 = 1$ in het platte vlak.



Laten we de 1 aan de rechterzijde vervangen door 22, dus $x^3 + y^3 = 22$. Het reële plaatje van $x^3 + y^3 = 22$ is, op een vergrotingsfactor na, hetzelfde als bovenstaande plaatje. Echter, nu zijn er wel oneindig veel rationale punten. De oplossing met kleinste noemers is $(25469/9954, 17299/9954)$. De variant $x^3 + y^3 = 4$, op zijn beurt, heeft weer geen oplossingen. Sommige getallen zijn dus wel som van twee rationale derde machten (dwz derde machten van rationale getallen), zelfs op oneindig veel manieren, anderen weer niet. Een dergelijk grillig gedrag, gecombineerd met de enorme moeilijkheidsgraad van de problemen, is voor de ene wiskundige een nachtmerrie en voor de ander een ultieme uitdaging.
Een ander succesverhaal, naast Wiles, is Mihailescu's bewijs van het vermoeden van Catalan in 2002. Neem de rij zuivere gehele machten (kwadraten, derde machten, vierde machten, ...). Deze begint met

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, \ldots$$

Het valt op dat het verschil tussen de achtereenvolgende getallen in deze rij

gemiddeld genomen toeneemt. Catalan formuleerde in 1844 het vermoeden dat de enige zuivere machten met onderling verschil 1 de getallen $2^3 = 8$ en $3^2 = 9$ zijn. Meer dan anderhalve eeuw bleef dit vermoeden onbewezen, totdat in 2002 Preda Mihailescu een bewijs van deze stelling gaf. Hoewel het niet de diepte en reikwijdte van Wiles' werk heeft, is dit toch een prestatie van formaat. Talloze wiskundigen voor Mihailescu waren er niet uitgekomen en vele van mijn vakgenoten hadden niet gedacht dit moment nog mee te mogen maken. Momenteel zijn er twee boeken over dit bewijs geschreven, maar helaas bestemd voor wiskundige experts. De methode maakt sterk gebruik van het verschil 1. Kijkend naar de rij zuivere machten zou men kunnen vermoeden dat $5^2 = 25$ en $3^3 = 27$ de enige machten zijn die 2 verschillen, maar niemand heeft enig idee hoe dit aan te pakken. Dezelfde opmerking geldt voor alle andere verschillen groter dan 1.
Terug naar Diophantus. In de rest van dit verhaal zullen we een voorbeeld uit de Arithmetica behandelen en daarbij iets laten zien van de enorme ingenieusiteit van Diophantus om een oplossing te geven. Daarna maken we een grote sprong in de tijd en beschrijven heel kort moderne pogingen om enige orde in de wereld van diophantische vergelijkingen te scheppen. Ondanks alle successen van de getaltheorie zal daarbij blijken dat veel problemen waar Diophantus mee worstelde nog steeds een probleem vormen. Men begint zich zelfs af te vragen of we met dit gebied een fundamentele scheidslijn benaderen van vragen die beantwoord kunnen worden en vragen waarop domweg geen antwoord bestaat. Bepalen waar die lijn precies ligt is de grote uitdaging.

2 Een probleem van Diophantus

Laten we eerst eens kijken naar twee vergelijkingen uit de inleiding, te beginnen met $x^2 - y^2 = 1$ in de rationale onbekenden x, y. We kunnen deze vergelijking herschrijven als $(x - y)(x + y) = 1$. Laten we $x + y$ aangeven met u. Dan volgt uit onze vergelijking dat $x - y = 1/u$. Dus

$$x + y = u, \qquad x - y = 1/u.$$

Hieruit leiden we gemakkelijk af dat

$$x = \frac{1}{2}\left(u + \frac{1}{u}\right), \qquad y = \frac{1}{2}\left(u - \frac{1}{u}\right).$$

Elke oplossing heeft dus deze gedaante. Omgekeerd gaat men eenvoudig na dat voor elke keuze van u de bijbehorende x, y voldoen aan $x^2 - y^2 = 1$. Het moet nu niet moeilijk zijn om de volgende algemenere vraag te beantwoorden.

Opgave 2.1 *Stel A is een geheel of rationaal getal ongelijk aan 0. Bepaal alle rationale oplossingen x, y van $x^2 - y^2 = A$.*

Hoewel het een beetje van onze hoofdlijn afwijkt is hier nog een opgave.

Opgave 2.2 *Stel A is een geheel getal. Als A oneven is, of deelbaar door 4, dan is A te schrijven als verschil van twee gehele kwadraten. Bewijs dit. Bewijs daarna dat in het overblijvende geval $A \equiv 2 (\mathrm{mod}\ 4)$ er geen oplossing is.*

Laten we nu overgaan naar de vraag $x^2 + y^2 = 1$ in de rationale getallen x, y. Stel $x \neq 0$ en deel aan beide zijden door x^2. We krijgen $1 + (y/x)^2 = (1/x)^2$, waaruit $(1/x)^2 - (y/x)^2 = 1$ volgt. Ons probleem is nu teruggebracht tot het schrijven van 1 als verschil van twee kwadraten. Er bestaat dus een rationaal getal u zo dat

$$\frac{1}{x} = \frac{1}{2}\left(u + \frac{1}{u}\right), \qquad \frac{y}{x} = \frac{1}{2}\left(u - \frac{1}{u}\right).$$

Hieruit leiden we af dat

$$x = \frac{2u}{u^2+1} \qquad y = \frac{u^2-1}{u^2+1}.$$

Dit is dus de algemene oplossing. Laten we een paar voorbeelden nemen. Kies $u = 3/10$ en we krijgen $(60/109)^2 + (91/109)^2 = 1$. Kies $u = 4/7$ en we krijgen $(56/65)^2 + (33/65)^2 = 1$. Het is trouwens aardig om uit deze gelijkheden de noemer weg te vermenigvuldigen. We krijgen $60^2 + 91^2 = 109^2$ en $56^2 + 33^2 = 65^2$, met andere woorden, oplossingen van de vergelijking $x^2 + y^2 = z^2$ in x, y, z geheel. Dit lukt uiteraard ook in het algemeen. Stel $u = r/s$ met r, s geheel en we vinden $x^2 + y^2 = z^2$ met $x = r^2 - s^2, y = 2rs, z = r^2 + s^2$.

Opgave 2.3 *Stel r, s geheel en $\mathrm{ggd}(r, s) = 1$ (dwz grootste gemeenschapelijke deler van r, s is 1). Stel $x = r^2 - s^2, y = 2rs, z = r^2 + s^2$. Laat zien dat $\mathrm{ggd}(x, y, z) = 1$ als $r \not\equiv s (\mathrm{mod}\ 2)$ en $\mathrm{ggd}(x, y, z) = 2$ als r, s beide oneven zijn.*

Dan nog een iets lastiger opgave ter vermaak.

Opgave 2.4 *Zij a, b, c een drietal gehele getallen zo dat $a^2 + b^2 = c^2$. Toon aan dat minstens een van deze getallen deelbaar is door 5.*

Konden we iedere rationale A schrijven als verschil van twee kwadraten van rationale getallen, voor sommen van twee rationale kwadraten lukt dat niet meer. Bijvoorbeeld $A = 3$. Stel er zijn rationale getallen x, y zo dat $x^2 + y^2 = A$. De kleinste gemeenschappelijke noemer van x, y geven we aan met c. Dus er zijn gehele a, b zo dat $x = a/c$ en $y = b/c$ en $\mathrm{ggd}(a, b, c) = 1$. Uit onze vergelijking volgt nu dat $a^2 + b^2 = 3c^2$. Bekijk deze vergelijking modulo 4. Omdat gehele kwadraten alleen 0 of 1 modulo 4 zijn, volgt hieruit dat $a^2 \equiv b^2 \equiv c^2 \equiv 0 (\mathrm{mod}\ 4)$. Dus a, b, c moeten even zijn en dit is in tegenspraak met onze voorwaarde dat $\mathrm{ggd}(a, b, c) = 1$. We concluderen dat er geen oplossingen bestaan.

Opgave 2.5 *Zij A een geheel getal dat $3 (\mathrm{mod}\ 4)$ is. Laat zien dat $x^2 + y^2 = A$ geen oplossing in rationale x, y heeft.*

De volgende opgave is wat lastiger.

Opgave 2.6 *Toon aan dat* 21 *geen som van twee rationale kwadraten is (hint: kijk modulo* 3*, of* 7*). Geef nog een ander geheel getal* A *dat* $1 \pmod 4$ *is, maar geen som van twee rationale kwadraten.*

Nadat we aldus warm gedraaid zijn, kunnen we naar een lastiger probleem van Diophantus kijken. Bovenstaande methoden waren trouwens in Diophantus tijd al gemeengoed en hij maakt er veelvuldig gebruik van. Hier is probleem 3 uit het Griekse Boek V van de Arithmetica in moderne taal opgeschreven.

Opgave 2.7 (Diophantus V.3) *Gegeven een getal* A *(niet nul), vindt drie rationale getallen zo dat elk van deze getallen alsmede hun producten vermeerderd met* A *een kwadraat opleveren. Anders gezegd, vindt rationale* x, y, z *zo dat*

$$\begin{aligned} x + A &= \square \\ y + A &= \square \\ z + A &= \square \\ xy + A &= \square \\ xz + A &= \square \\ yz + A &= \square \end{aligned}$$

De notatie $\square$ (kwadraat) spreekt hopelijk voor zich. Diophantus zelf gebruikte trouwens de notatie Δ^Υ voor kwadaten (en K^Υ voor derde machten, $\Delta^\Upsilon\Delta$ voor vierde machten, ΔK^Υ voor vijfde machten en $K^\Upsilon K$ voor zesde machten).
Laten we ter illustratie van Diophantus oplossing het voorbeeld $A = 1$ nemen. Tegenwoordig zouden we meteen de flauwe oplossing $x = y = z = 0$ opmerken. Diophantus werkte echter impliciet met positieve getallen en dus doen wij dit ook in dit voorbeeld. Alvorens te beginnen is het misschien goed om te kijken of een oplossing meteen te zien is. Als dat na enige tijd niet gelukt is, hebben we daarna des te meer respect voor Diophantus' oplossing. Het is belangrijk om te weten dat Diophantus tevreden was als hij 1 oplossing had gegeven. Blijkbaar was dit een illustratie want zijn methoden waren meestal voor uitbreiding vatbaar. Diophantus streefde er niet naar om een volledige oplossingsverzameling te vinden, zoals we dat tegenwoordig graag willen.
Zoals gezegd, we kiezen $A = 1$ en volgen Diophantus. Noem het eerste kwadraat t^2 en stel dat het tweede kwadraat $(t + 1)^2$ is. Dat wil zeggen dat $x = t^2 - 1$ en $y = (t + 1)^2 - 1 = t^2 + 2t$. Het slimme van Diophantus keuze is dat nu ook $xy + 1$ een kwadraat is, namelijk $xy + 1 = (t^2 - 1)(t^2 + 2t) + 1 = (t^2 + t - 1)^2$. Daarmee zouden we het probleem $x + A = \square, y + A = \square, xy + A = \square$ hebben opgelost. Blijkbaar was dit te eenvoudig naar Diophantus' smaak en heeft hij er een interessanter opgave van gemaakt door er nog een derde getal z bij te halen. Diophantus merkt nu op dat als we $z = 2(x + y) - 1 = (2t + 1)^2 - 4$ nemen, ook de getallen $xz+1$ en $yz+1$ kwadraten zijn, namelijk $(2t^2+t-2)^2$ en $(2t^2 + 3t - 1)^2$ zoals men zelf gemakkelijk kan narekenen. De enige vergelijking die overblijft is $z + 1 = \square$, ofwel $(2t + 1)^2 - 3 = s^2$ voor zekere s. Het probleem is nu teruggevoerd tot het schrijven van 3 als verschil van twee kwadraten, een

techniek die we nu beheersen. Uit opgave 2.1 weten we dat er een u bestaat zo dat $2t+1 = \frac{1}{2}(u+3/u)$. Kies bijvoorbeeld $u = 1/2$. We vinden $t = 9/8$ en

$$x = \frac{17}{64}, \quad y = \frac{225}{64}, \quad z = \frac{105}{16}.$$

Uiteraard kunnen we oneindig veel oplossingen maken door oneindig veel verschillende waarden voor u te nemen. We moeten daarbij wel oppassen dat $t > 1$ blijft, anders wordt x negatief.
Het opmerkelijke van Diophantus' methode is dat hij voor alle waarden van A werkt, dus niet alleen $A = 1$. In de Arithmetica geeft Diophantus een oplossing bij $A = 5$,

$$x = \frac{2861}{676}, \quad y = \frac{7645}{676}, \quad z = \frac{20336}{676}.$$

Opgave 2.8 *Vindt een oneindige serie oplossingen voor Diophantus' opgave 2.7 met $A = 2$.*

Laten we Diophantus' opgave nog eens opschrijven, nu met de kwadraten expliciet opgeschreven,

$$\begin{aligned} x + A &= p^2 \\ y + A &= q^2 \\ z + A &= r^2 \\ xy + A &= u^2 \\ xz + A &= v^2 \\ yz + A &= w^2 \end{aligned}$$

Tgenwoordig zouden we het probleem als volgt aanpakken. We zien dat $x = p^2 - A, y = q^2 - A, z = r^2 - A$. Vul deze in de laatste drie vergelijkingen in en we krijgen het stelsel

$$\begin{aligned} (p^2 - A)(q^2 - A) + A &= u^2 \\ (p^2 - A)(r^2 - A) + A &= v^2 \\ (q^2 - A)(r^2 - A) + A &= w^2 \end{aligned}$$

in de onbekende breuken p, q, r, u, v, w. In plaats van één diophantische vergelijking hebben we nu een stelsel diophantische vergelijkingen gekregen. Als men wil kan men daar weer 1 diophantische vergelijking van maken, maar we zullen dat hier niet doen. Diophantus vond één of meer oplossingen voor zijn problemen en was daar tevreden mee. Tegenwoordig rusten wij niet voordat we de gehele oplossingsverzameling gevonden hebben. Maar helaas, ondanks alle technieken die tussen Diophantus' tijd en nu gevonden zijn, is het totaal niet duidelijk hoe bovenstaand probleem moet worden aangepakt. Hier is nog een ander probleem uit de Arithmetica.

Opgave 2.9 (Diophantus, V.27) *Gegeven een getal A, vindt drie kwadraten zo dat de som van elk tweetal plus A weer een kwadraat is.*

Laten we het geval $A = 0$ eens opschrijven,

$$\begin{array}{ccccccc} a^2 & + & b^2 & & & = & \square \\ a^2 & & & + & c^2 & = & \square \\ & & b^2 & + & c^2 & = & \square \end{array}$$

Meetkundig kunnen we dit probleem opvatten als vragen naar een rechthoeking blok met rationale zijden a, b, c waarvan de zijvlaksdiagonalen ook rationale lengte hebben. Diophantus' methode komt grofweg neer op het volgende. Leg één van de zijden vast, zeg $c = 1$. Dan komen de tweede en derde vergelijking weer neer op het schrijven van 1 als verschil van twee kwadraten. Laten we $a = \frac{1}{2}(u - 1/u)$ en $b = \frac{1}{2}(v - 1/v)$ kiezen. Stel $v = -tu$. De eerste vergelijking wordt

$$\frac{1}{4}\left(u - \frac{1}{u}\right)^2 + \frac{1}{4}\left(\frac{u}{t} - \frac{t}{u}\right)^2 = \square.$$

Uitwerken geeft

$$\left(\frac{1}{t^2} + 1\right) u^2 - 4 + (t^2 + 1)\frac{1}{u^2} = \square.$$

Om ervoor te zorgen dat de linkerzijde een kwadraat wordt, willen we t, u zodanig kiezen dat $4 = (t^2 + 1)/u^2$. Met andere woorden, $4u^2 = t^2 + 1$. En alweer moeten we 1 als verschil van twee kwadraten schrijven, $(2u)^2 - t^2 = 1$. Diophantus maakt hier de specifieke keuze $t = 3/4$, maar wij kiezen $t = (\tau - 1/\tau)/2$. Voor u kunnen we dan $u = (\tau + 1/\tau)/4$ nemen. Vervolgens vinden we $v = -ut = (\tau^2 - 1/\tau^2)/8$ en voor a, b,

$$\begin{aligned} a &= \frac{1}{2}(u - 1/u) = \frac{t^4 - 14t^2 + 1}{8t(t^2 + 1)} \\ b &= \frac{1}{2}(v - 1/v) = \frac{3t^4 - 10t^2 + 3}{4(t^4 - 1)} \\ c &= 1 \end{aligned}$$

Als we alle zijden van ons gevonden blok vermenigvuldigen met $8t(t^4 - 1)$ krijgen we de oplossingen

$$\begin{aligned} a &= t^6 - 15t^4 + 15t^2 - 1 \\ b &= 6t^5 - 20t^3 + 6t \\ c &= 8t^5 - 8t \end{aligned}$$

We mogen t hierin willekeurig rationaal kiezen. Door de keuzen die we gemaakt hebben is dit natuurlijk niet de volledige oplossingsverzameling, net zo min als dat bij Diophantus het geval is. Naast bovenstaande oplossing zijn er nog vele andere series oplossingen gevonden, er zijn zelfs oneindig veel van dit soort series. Helaas is de volledige oplossingsverzameling nog steeds niet bekend.
Tenslotte, om de zaak nog spannender te maken, kunnen we aan ons stelsel de extra eis $a^2 + b^2 + c^2 = \square$ toevoegen. Meetkundig vragen we dan naar een rechthoekig blok met (positieve) rationale zijden waarvan alle diagonalen,

zowel zijvlaksdiagonalen als lichaamsdiagonaal, ook rationale lengte hebben. Een dergelijk blok noemen we *rationale cuboide*. Tot op de dag van vandaag is het niet bekend of rationale cuboiden al of niet bestaan.

Opgave 2.10 *Geef een oplossing met drie verschillende getallen a, b, c van opgave 2.9 voor $A = 1$,*

$$\begin{array}{ccccccccc} a^2 & + & b^2 & & & + & 1 & = & \square \\ a^2 & & & + & c^2 & + & 1 & = & \square \\ & & b^2 & + & c^2 & + & 1 & = & \square \end{array}$$

3 Stand van zaken

Uiteraard is er sinds Diophantus veel gebeurd op het gebied van diophantische vergelijkingen. De technieken van Diophantus bestonden uit eenvoudige algebra die op buitengewoon slimme manier werden ingezet. Tegenwoordig beschikken we over een veel ruimer arsenaal aan technieken. Zonder uit te leggen wat ze precies betekenen noemen we hier de belangrijkste.

- Algebraïsche meetkunde. Dit is het gebied dat de reëel- of complex-meetkundige eigenschappen van de objecten gegeven door vergelijkingen $F(x_1, \ldots, x_n) = 0$ bestudeerd. Alvorens een diophantische vergelijking op te lossen is het goed om eerst de meetkundige structuur te kennen. Men zou kunnen zeggen dat Diophantus' aanpak een eenvoudige vorm van algebraïsche meetkunde is, hoewel Diophantus zelf nooit meetkundige termen gebruikt.

- Algebraïsche getaltheorie. Deze tak van de getaltheorie ontstond uit pogingen halverwege de 19e eeuw om Fermat's vermoeden op te lossen. Echter, de toepassingsmogelijkheden van de algebraïsche getaltheorie zijn veel breder.

- Diophantische approximatie en transcendentietheorie, vanaf het begin van de twintigste eeuw ontwikkeld. Het zijn deze technieken die, in combinatie met algebraische methoden, tot nu toe het meest succesvol zijn gebleken in de volledige oplossing van speciale diophantische vergelijkingen.

- Galoisrepresentaties. Deze tak van de getaltheorie is pas tot volle ontwikkeling gekomen vanaf de tweede helft van de vorige eeuw. Toepassingen op diophantische vergelijkingen vonden pas plaats vanaf de 80-er jaren. De meest spectaculaire is de oplossing van Fermat's vermoeden door A. Wiles.

Naast resultaten zijn er ook veel vermoedens geformuleerd over de oplossingsverzameling van een diophantische vergelijking. De meest vergaande zijn de zogenaamde *Vojta vermoedens*. Deze geven een mooie systematiek in de aard van oplossingsverzamelingen van diophantische vergelijkingen. Helaas zijn dit

slechts vermoedens en ligt het bewijs ervan waarschijnlijk in een nog verre toekomst.
Om toch een idee te geven van de systematiek van diophantische vergelijkingen geven we een korte bloemlezing over diophantische vergelijkingen in twee en drie variabelen. Voor iets uitgebreidere informatie verwijzen we naar F. Beukers, *Getaltheorie voor beginners*, Hoofdstukken 12.4, 13, 15, 16 en 17.

Twee variabelen

De algemene vorm is $F(x,y) = 0$ in rationale x, y, waarbij F een polynoom is in twee variabelen en met gehele coëfficiënten. Meetkundig gezien stelt deze vergelijking een algebraische kromme voor, denk maar aan $x^2 + y^2 = 1$ (cirkel) of $xy = 1$ (hyperbool). We sorteren onze vergelijkingen eerst naar hun totale graad.
Vergelijkingen van graad 1 hebben we de vorm $ax + by = c$. De bepaling van rationale punten hierop is simpel. We kiezen gewoon een rationale x en berekenen $y = (c - ax)/b$.

graad 2

Vergelijkingen van graad 2 zien er uit als

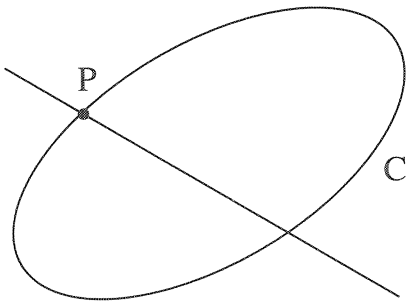
$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

waarin $a, b, c, d, e, f \in \mathbb{Z}$ gegeven zijn. Meetkundig levert deze vergelijking ons een ellips, parabool, hyperbool of een tweetal rechte lijnen op. We noemen dergelijke krommen *kegelsneden*. Bijvoorbeeld $x^2 + 2y^2 = 1$ (ellips) of $y = 2x^2$ (parabool) of $xy = 1$ (hyperbool) of $(x+y-1)(x+2y) = 0$ (paar rechte lijnen). Het geval dat de kegelsnede uit twee lijnen bestaat noemen we *reducibel*. De andere gevallen noemen we *irreducibel*. Soms krijgen we de lege verzameling zoals bij $x^2 + y^2 + 1 = 0$.
Laten we eerst eens kijken hoe het zit met de rationale oplossingen, dat wil zeggen punten (x, y) op de kegelsnede met rationale x, y. We geven hier de stelling en een voorbeeld hoe we eraan komen. We zullen hier het taalgebruik bezigen dat we een rationale oplossing van de vergelijking een rationaal punt op de kegelsnede noemen en een geheeltallige oplossing een geheel punt op de kegelsnede.

Stelling 3.1 *Stel a, b, c, d, e, f geheel en stel dat de kegelsnede $ax^2+bxy+cy^2+dx+ey+f = 0$ irreducibel is en een rationaal punt bevat. Dan bevat hij oneindig veel rationale punten.*

Deze stelling berust op het feit dat het heel eenvoudig is om, uitgaand van een rationaal punt, andere rationale punten te construeren. Noem de kegelsnede C en het rationale punt P. Kies een willekeurige rechte lijn l door P waarvan de helling rationaal is. Deze lijn snijdt de kegelsnede C in twee punten. Een ervan kennen we al, dat is P. Het andere punt blijkt ook rationaal te zijn. Door de helling van l te variëren kunnen we op deze manier alle rationale punten op C vinden.

Hier is een voorbeeld. Beschouw de kromme $x^2 + 3y^2 - 5x + 1 = 0$. Het is duidelijk dat $x = 1, y = 1$ een rationaal punt is. Trek een willekeurige rechte door $(1, 1)$ met rationale helling. Deze heeft de vorm $y = 1 + t(x - 1)$ met t rationaal. Snijdt deze lijn met $x^2 + 3y^2 - 5x + 1 = 0$.



We vinden,

$$\begin{aligned} 0 &= x^2 + 3(1 + t(x-1))^2 - 5x + 1 \\ &= x^2 - 5x + 4 + 6t(x-1) + 3t^2(x-1)^2 \\ &= (x-1)(x-4) + 6t(x-1) + 3t^2(x-1)^2. \end{aligned}$$

Eén oplossing kennen we al, $x = 1$, vanwege het punt $P = (1, 1)$. De x-coördinaat van het andere snijpunt wordt $x = (4 - 6t + 3t^2)/(1 + 3t^2)$. De bijbehorende waarde van y is $y = (1 + 3t - 3t^2)/(1 + 3t^2)$. Het resultaat is dat $x = (4 - 6t + 3t^2)/(1 + 3t^2), y = (1 + 3t - 3t^2)/(1 + 3t^2)$ voor willekeurige rationale t een oplossing van $x^2 + 3y^2 - 5x + 1 = 0$ is. Neem bijvoorbeeld $t = 5/4$, waarmee we $x = 19/91, y = 1/91$ vinden. De oplossingen kunnen er dus best spectaculair uitzien. We noemen deze methode de *koordenmethode.*

Opgave 3.2 *Gebruik de koordenmethode met het punt* $(1, 0)$ *om de oplossingen van* $x^2 + y^2 = 1$ *in rationale* x, y *te vinden.*

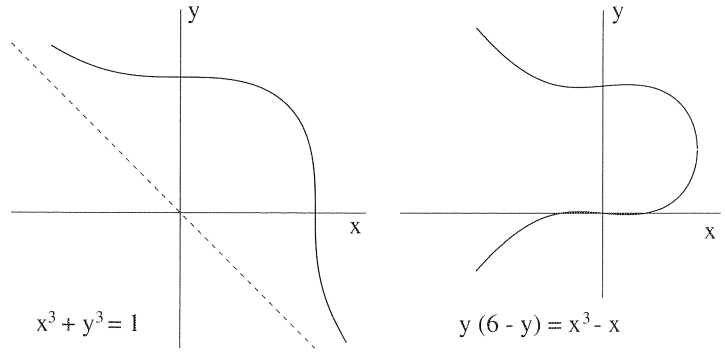
Opgave 3.3 *Gebruik de koordenmethode om de oplossingen van* $x^2 - 3xy + 3y^2 - x - y = 0$ *in rationale* x, y *te vinden.*

Tenslotte zij opgemerkt, dat er ook kegelsneden zijn met gehele coëfficiënten waarop helemaal geen rationale punten liggen, zoals $x^2 + y^2 = -1$ (hopelijk duidelijk) of $x^2 + y^2 = 3$, die we eerder hebben uitgewerkt.
Over gehele oplossingen van kwadratische vergelijkingen in twee variabelen bestaan ook resultaten, maar daarvoor verwijzen we naar F. Beukers, *Getaltheorie voor Beginners*, Hoofdstuk 16.3.

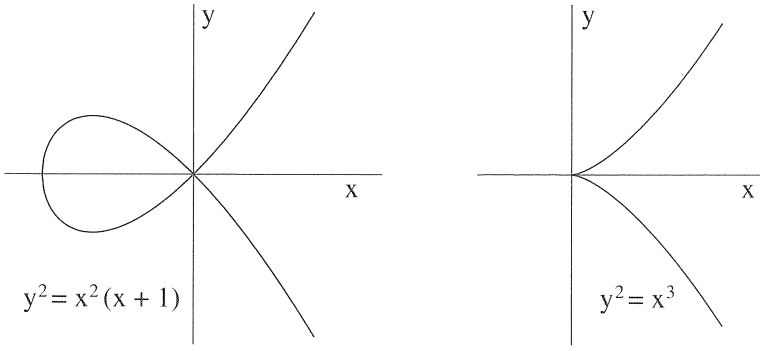
graad 3
Dit is het geval van de vergelijking

$$a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3 + a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00} = 0$$

waarin de a_{ij} gehele gegeven getallen zijn en x, y, zoals gewoonlijk, de onbekenden. Neem even aan dat niet alle coëfficiënten nul zijn. De punten gedefinieerd door deze vergelijking noemen we een cubische kromme en we zullen hem C noemen. In deze paragraaf beperken we ons tot *niet-singuliere* krommen C. Het zou iets te ver voeren om hier precies te omschrijven wat ermee bedoeld wordt. Grof gezegd betekent het dat de kromme geen singuliere punten bevat, ook niet in het 'oneindige'. Hier zijn een paar voorbeelden,

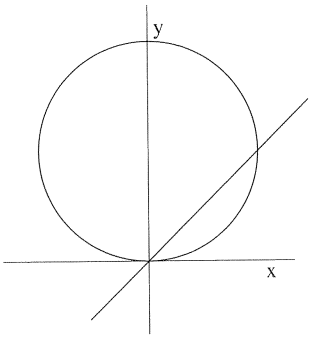


Een punt op de kromme C heet singulier als de kromme in dat punt geen unieke raaklijn heeft. De volgende voorbeelden hebben een singulier punt in $(0, 0)$.

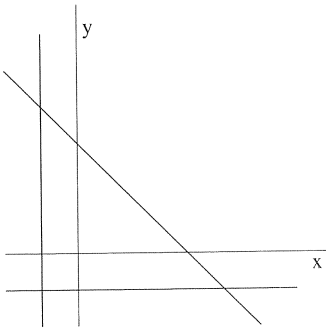


Vervolgens zijn ook de reducibele krommen, dat wil zeggen krommen die uit meerdere deelkrommen bestaan, singulier. Zoals $(y - x)(x^2 + y^2 - y) = 0$ en $(x + 1)(y + 1)(x + y - 3) = 0$,
We zullen ons verder alleen beperken tot niet-singuliere cubische krommen, ook wel *elliptische kromme* genoemd, hoewel ze verder helemaal niets met ellipsen te maken hebben. Het is een naam die historisch zo gegroeid is.

Het bekendste voorbeeld van een elliptische kromme is $y^2 = x^3 + ax^2 + bx + c$ waarin het polynoom x^3+ax^2+bx+c geen meervoudige nulpunten mag hebben.

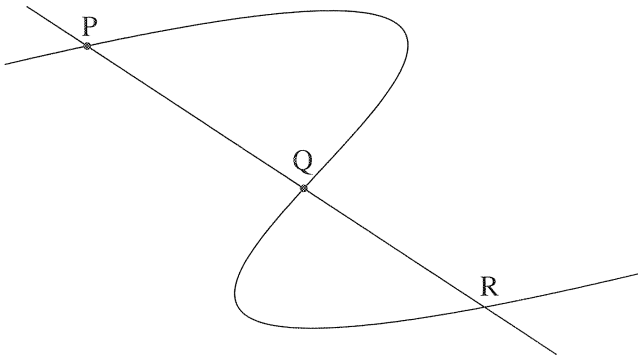


$(x - y)(x^2 + y^2 - y) = 0$



$(x + 1)(y + 1)(x + y - 3) = 0$

De studie van rationale punten op elliptische krommen is één van de verst ontwikkelde takken van de theorie van de diophantische vergelijkingen. De afgelopen 30 jaar heeft dit onderwerp een enorme ontwikkeling doorgemaakt en een deel van deze ontwikkeling heeft geculmineerd in het bewijs van de Laatste Stelling van Fermat, zie F. Beukers, *Getaltheorie voor Beginners*, Hoofdstuk 13. Uiteraard kunnen wij niet op al deze ontwikkelingen ingaan. Het staat wel vast dat de eerste technieken om oplossingen te vinden in primitieve gedaante al aan Diophantus en Fermat bekend waren. We geven een schets van deze oplossingsmethode en daarna een voorbeeld. Het idee gaat als volgt. Beschouw de cubische kromme C en stel dat we twee rationale punten P en Q op C hebben.



Verbind deze twee punten door een rechte lijn l. Aangezien in het algemeen een rechte lijn een cubische kromme in drie punten snijdt, bevat $l \cap C$ naast P en Q nog een derde snijpunt dat we R noemen. Het blijkt dat dit ook een rationaal punt is en op deze manier kunnen we uit bestaande rationale punten nieuwe rationale punten maken.
Er is ook een variant mogelijk waarin we met één rationaal punt P op C beginnen. Trek vervolgens de raaklijn l door P aan de kromme C. Dan snijdt l de kromme C tweevoudig in het punt P en enkelvoudig in een derde punt dat we

weer R noemen. Het blijkt dat R weer een rationaal punt is.
Bovenstaande constructie noemen we de *koorde-raaklijn constructie*. Door deze constructie herhaald uit te voeren, kunnen oneindig veel rationale punten op C vinden, mits ze bestaan.
Laten we de koorde-raaklijn methode eens aan de hand van een voorbeeld uitvoeren. Beschouw de vergelijking $x^3 + y^3 = 1729$. Tussen haakjes, men kan opmerken dat 1729 het kleinste positieve getal is dat op meer dan één manier als som van twee gehele derde machten geschreven kan worden, namelijk $1729 = 1^3 + 12^3 = 10^3 + 9^3$. Dit geeft ons meteen een tweetal oplossingen van onze vergelijking. We gaan nu andere rationale oplossingen construeren.
Bepaal de rechte lijn die door de twee punten $(1, 12)$ en $(10, 9)$ gaat, $y = -x/3 + 37/3$. Snijd deze met de kromme $x^3 + y^3 = 1729$. We verwachten hierbij drie snijpunten, omdat een rechte lijn een derdegraads kromme (cubische kromme) in het algemeen in drie punten snijdt. Twee snijpunten kennen we al, $(10, 9)$ en $(1, 12)$. We willen graag het derde snijpunt bepalen. Dit kunnen we doen door bijvoorbeeld y uit beide vergelijkingen te elimineren. We krijgen,

$$x^3 + (-x/3 + 37/3)^3 = 1729.$$

Na uitwerking,

$$\frac{26}{27}x^3 + \frac{37}{9}x^2 - \frac{1369}{9}x + \frac{3970}{27} = 0.$$

We vermenigvuldigen dit met $27/26$ om de coëfficiënt van x^3 gelijk aan 1 te maken en vinden,

$$x^3 + \frac{111}{26}x^2 - \frac{4107}{26}x + \frac{3970}{26} = 0.$$

Twee oplossingen van deze vergelijking kennen we al, dat zijn $x = 10$ en $x = 1$. Na wegdeling van de factoren $(x - 1)(x - 10)$ houden we over, $x + \frac{397}{26} = 0$. Dus de x-coördinaat van het derde snijpunt is $x = -397/26$ en de bijbehorende y-coördinaat is $y = -x/3 + 37/3 = 453/26$. Controle leert inderdaad dat

$$\left(\frac{-397}{26}\right)^3 + \left(\frac{453}{26}\right)^3 = 1729.$$

Om rekenwerk te besparen hadden we derde graadsvergelijking niet door $(x - 1)(x - 10)$ hoeven delen. We hadden simplweg kunnen opmerken dat minus het product van de drie oplossingen gelijk is aan $3970/26$, de constante term in onze cubische vergelijking. Twee ervan kennen we al, 1 en 10, en blijft dus over minus $3970/26$ gedeeld door 10, en dat is $-397/26$.
Aangemoedigd door het succes van deze constructie kunnen we natuurlijk proberen nog een punt te vinden door $(1, 12)$ en $(-397/26, 453/26)$ op analoge wijze te combineren. Helaas vinden we dan weer het oude punt $(10, 9)$. *Waarom?* Maar geen nood, $(453/26, -397/26)$ (coördinaten verwisselen) is ook een punt op onze kromme en combinatie met $(1, 12)$ levert inderdaad weer een nieuw punt, te weten

$$(2472830/187953, -1538423/187953).$$

Zo doorgaand kan men oneindig veel rationale oplossingen van $x^3 + y^3 = 1729$ vinden.
In plaats van een verbindingsrechte tussen twee punten kunnen we ook de raaklijn aan de kromme in een punt, zeg $(1, 12)$ nemen. In het algemeen wordt de raaklijn aan $x^3+y^3 = A$ in het punt $P = (x_0, y_0)$ gegeven door $x_0^2x+y_0^2y = A$. In ons geval krijgen we $x + 144y = 1729$. Deze raaklijn snijdt de kromme in $(1, 12)$ (dubbel) en in een ander punt. De berekening van dit laatste punt gaat op dezelfde manier als daarnet. Eliminatie van y geeft $x^3 + (1729 - x)^3/144^3 = 1729$ en na uitwerking,

$$\frac{2985983}{2985984}x^3 + \frac{1729}{995328}x^2 - \frac{2989441}{995328}x + \frac{5977153}{2985984} = 0$$

Na vermenigvuldiging met $\frac{2985984}{2985983}$ vinden we

$$x^3 + \frac{3}{1727}x^2 - \frac{5187}{1727}x + \frac{3457}{1727} = 0.$$

Een dubbele oplossing kennen we al, $x = 1$. Na wegdeling van de factor $(x-1)^2$ houden we over, $x + \frac{3457}{1727} = 0$. Dus $x = -\frac{3457}{1727}$ en de bijbehorende y-waarde is $y = (1729 - x)/144 = \frac{20760}{1727}$. Controle levert dat inderdaad

$$\left(-\frac{3457}{1727}\right)^3 + \left(\frac{20760}{1727}\right)^3 = 1729.$$

Opgave 3.4 *Beschouw de diophantische vergelijking $y^2 = x^3 + 17$ in rationale onbekenden x, y. De oplossingen $P = (-1, 4)$ en $Q = (-2, 3)$ zijn makkelijk te zien.*

1. *Probeer voor alle gehele x met $|x| < 10$ of er een bijbehorende gehele y bestaat zo dat $y^2 = x^3 + 17$.*

2. *Bepaal de lijn door P, Q en snijdt deze met de kromme $y^2 = x^3 + 17$. Bepaal het derde snijpunt R.*

3. *Verander het teken van de y-coördinaat in R en herhaal de constructie met dit nieuwe punt en Q.*

4. *Construeer nog een paar punten met de reeds gevonden punten. Een klein computerprogramma kan hier erg behulpzaam zijn.*

5. *Bepaal het derde snijpunt van de raaklijn in Q met $y^2 = x^3 + 17$. Doe hetzelfde met de raaklijn in P.*

Wat betreft *gehele* oplossingen van derde graadsvergelijkingen in twee variabelen is er een diepe stelling van C.L. Siegel uit 1929, zie Stelling 3.5.

graad $\geq$4 Het zal duidelijk zijn dat naarmate de graad van een diophantische vergelijking groter wordt, de kans dat er oplossingen zijn, rationale of gehele, steeds kleiner wordt. Het blijkt dat de graad van een vergelijking niet altijd

een goede indicatie geeft van de complexiteit van de bijbehorende kromme. Een veel betere graadmeter is het zogenaamde *geslacht* van een kromme. Daarmee bedoelen we niet het geslacht in biologische zin, maar een geheel getal $g \geq 0$ dat we aan iedere kromme $F(x, y) = 0$ kunnen toekennen. Het is lastig om hier uit te leggen hoe dit geslacht precies gedefinieerd is. Daarvoor verwijzen we naar de boeken over algebraïsche meetkunde. We volstaan hier met de opmerking dat als een kromme van graad n geen singuliere punten heeft, dan is het geslacht gelijk aan $g = (n-1)(n-2)/2$. Dit betekent dat kegelsneden ($n = 2$) geslacht $1 \cdot 0/2 = 0$ hebben en elliptische krommen ($n = 3$) geslacht $2 \cdot 1/2 = 1$. Een niet-singuliere vierde graadskromme daarentegen heeft geslacht $3 \cdot 2/2 = 3$.
Er zijn twee hoofdresultaten die behoren tot de belangrijkste resultaten op het gebied van diophantische vergelijkingen. De allereerste is van C.L. Siegel.

Stelling 3.5 (Siegel, 1929) *Een kromme van geslacht $g > 0$ bevat hoogstens eindig veel geheeltallige punten.*

In de vorige paragraaf hebben we gezien dat een elliptische kromme ($g = 1$) oneindig veel rationale punten kan bevatten. Echter, in de twintiger jaren vermoedde L.J. Mordell al dat een kromme van geslacht $g > 1$ hooguit eindig veel rationale punten bevat. Dit vermoeden gold jarenlang als buitengewoon lastig tot in 1983 G. Faltings een bewijs gaf.

Stelling 3.6 (Faltings, 1983) *Zij C een algebraïsche kromme van geslacht $>$ 1. Dan bevat C hooguit eindig veel rationale punten.*

Het bewijs van deze stelling is echter nog steeds lastig en berust op zeer diepe methoden uit de arithmetisch algebraïsche meetkunde.
De stellingen van Siegel en Faltings zijn stellingen die de eindigheid van de oplossingsverzameling geven. Ze geven echter geen enkele methode om eventuele oplossingen ook inderdaad te vinden. Er is wel een aantal standaardtypen van vergelijkingen dat routine-matig kan worden opgelost. Hierbij worden vaak technieken gebruikt die pas in de 70-er jaren beschikbaar kwamen. Vergelijkingen die afwijken van deze standaardtypen kunnen buitengewoon lastig zijn. Om een paar dramatische voorbeelden te noemen, er is een artikel van 9 bladzijden met lastige technieken voor nodig om aan te tonen dat $2^4 + 1^4 = 17$ de enige rationale oplossing (op verwisseling en tekenwisseling na) van $x^4 + y^4 = 17$ is. Een ander voorbeeld, in de Arabische versie van de Arithmetica staat als probleem VI.17 de vraag om $y^2 = x^6 + x^2 + 1$ op te lossen in rationale x, y. Dat de enige oplossingen $(0, \pm 1)$ en $(1/2, \pm 9/8)$ zijn, was het onderwerp van het proefschrift van J.Wheterall in 1998. Men zou kunnen zeggen dat dit tot nu het langst open staande probleem in de geschiedenis van de wiskunde is geweest.

Drie variabelen

Deze vergelijkingen zien er als volgt uit

$$F(x, y, z) = 0$$

waarin F een polynoom met gehele coëfficiënten is. Meetkundig gezien hebben we hier met de vraag te maken of een gegeven oppervlak gehele of rationale

punten bevat. Denk bijvoorbeeld aan de vergelijking $x^2+y^2+z^2 = 1$ in rationale x, y, z. Anders gezegd, bepaal alle punten met rationale coördinaten op een bol met straal 1. We geven een korte ordening naar graad.

graad 2
In het algemeen ziet deze er uit als

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + a_{12}xy + a_{13}xz + a_{23}yz + b_1x + b_2y + b_3z + c = 0$$

in de rationale onbekenden x, y, z. Vergelijkingen van dit type kunnen op dezelfde manier worden aangepakt als kwadratische vergelijkingen in twee variabelen. Kies namelijk een rationaal punt P op dit kwadratische oppervlak. Construeer vervolgens een rechte lijn l door P en bepaal het tweede snijpunt. Omdat de richting van l vastgelegd door twee parameters kunnen we een parametrisatie met twee parameters verwachten.

Opgave 3.7 *Pas deze methode toe op de vergelijking $x^2 + y^2 + z^2 = 1$ en het punt $P = (0, 1)$.*

Opgave 3.8 *Toon aan dat de vergelijking $x^2 + y^2 + z^2 = 7$ in rationale x, y, z geen oplossingen heeft.*

graad 3
Het oppervlak $F(x, y, z) = 0$ noemen we een cubisch oppervlak. Bepaling van rationale punten op een cubisch oppervlak kan lastig zijn. Wel hebben we de volgende stelling.

Stelling 3.9 (Segre, 1946) *Zij $F(x, y, z) = 0$ een cubisch oppervlak. Als er 1 rationaal punt op ligt dan liggen er oneindig veel op.*

De methode om deze stelling te bewijzen gaat geheel via een aantal meetkundige constructies. Met enige fantasie zou men kunnen zeggen dat deze methode bij Diophantus' aanpak aansluit. We laten nu een voorbeeld zien van oppervlakken met oneindig veel rationale punten. Misschien is het leuk om te weten dat deze werd gevonden door een schoolmeester uit Engeland.

Stelling 3.10 (Riley, 1825) *Voor elke gehele n zijn er oneindig veel positieve rationale drietallen x, y, z zó dat $x^3 + y^3 + z^3 = n$.*

Om deze stelling te zien, kies

$$A = \frac{12t - (t+1)^2}{6(t+1)}, \quad B = \frac{(t+1)^3 - 12t(t-1)}{6(t+1)^2}, \quad C = \frac{2t(t-1)}{(t+1)^2}$$

en merk op dat $A^3 + B^3 + C^3 = t/3$. Kies $t = 3nu^3$ met u rationaal, zelf te kiezen zó dat $1 < 3nu^3 < 2$. Vul vervolgens deze t in A, B, C in deel alle drie door u. De derde machten van de zo gevormde getallen hebben als som n. De ongelijkheid $1 < 3nu^3 < 2$ zorgt ervoor dat de gevonden getallen positief worden. Als men tevreden is met eventueel negatieve getallen dan kan het ook zonder deze voorwaarde.

Opgave 3.11 *Gebruik de zojuist gegeven methode om* 11 *als som van drie positieve rationale derde machten te schrijven.*

graad $\geq$4
We komen nu op een gebied waar weinig bekend is. Er zijn nauwelijks oppervlakken van graad ≥ 4 waarvan men de verzameling rationale punten kent. Technieken om dit soort vergelijkingen aan te pakken zijn er ook nauwelijks. Ter illustratie, Euler vermoedde in de 18e eeuw dat de vergelijking $1 = x^4 + y^4 + z^4$ in rationale x, y, z alleen triviale oplossingen zoals $1 = 1^4 + 0^4 + 0^4$ heeft. Het heeft tot 1988 geduurd voordat N. Elkies het tegendeel aantoonde. Er bestaan zelfs oneindig veel oplossingen. De "kleinste"niet-triviale is

$$\left(\frac{95800}{422481}\right)^4 + \left(\frac{217519}{422481}\right)^4 + \left(\frac{414560}{422481}\right)^4 = 1.$$

Het bewijs van Elkies' resultaat is een ingenieuze combinatie van meetkundige methoden en een aantal gelukkige omstandigheden.
We zijn hiermee aan de grens van onze mogelijkheden gekomen om diophantische vergelijkingen aan te pakken. Dat we daarmee langzaam maar zeker een grens naderen waarin de aanpak van diophantische vergelijkingen ook fundamenteel onmogelijk is, zal uit de volgende paragraaf blijken.

4 Hilbert's tiende probleem

Tijdens het Wereld Mathematisch Congres in 1900 te Parijs hield één van de bekendste wiskundigen uit die tijd, David Hilbert, een voordracht over wat hij dacht dat de grote wiskundeproblemen voor de komende eeuw zou zijn. De volledige tekst is te vinden op de website
`www.mathematik.uni-bielefeld.de/~kersten/hilbert/rede.html`
Hilbert's lijst bestond uit 23 problemen, die allemaal een zekere status hebben gekregen, mede doordat ze in deze lijst voorkomen. Sommigen zijn inmiddels opgelost, anderen niet. Een voorbeeld van een onopgelost probleem is Hilbert's probleem 8: de zogenaamde *Riemann hypothese.* Deze komt ook voor in de lijst van *Clay Prize problems*, de grote wiskunde problemen voor het nieuwe millenium, ditmaal met een prijzengeld van 1.000.000 US dollar per probleem. Zie de website `www.claymath.org/millennium`.
Het 10e Hilbertprobleem is voor ons van belang. In Hilbert's woorden:

Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Hoewel Hilbert het misschien niet zo formuleerde kwam zijn vraag neer op de vraag of er een methode bestaat om van een willekeurige diophantische vergelijking te beslissen of deze wel of geen oplossingen heeft. Om deze vraag goed te kunnen beantwoorden moeten we ons eerst afvragen wat er verstaan wordt

onder een 'methode' of 'algoritme'. In de eerste helft van de 20e eeuw is diep nagedacht over berekenbaarheid, algoritmen en de onderliggende logica. Een van de pioniers op dit gebied was Alan Turing, die de Turingmachine voorstelde als universeel instrument om algoritmen uit te voeren. Tegenwoordig hebben we allemaal een Turingmachine op ons bureau staan, namelijk de gewone computer. Iets preciezer: een Turingmachine is een computer met onbeperkt geheugen. Onze computers hebben altijd een begrensde hoeveelheid geheugen, maar het zal niet moeilijk zijn om er een met onbeperkt geheugen voor te stellen. Immers, elke keer als we meer geheugen nodig hebben kopen we er gewoon wat bij. In deze opvatting is een algoritme (of 'methode') niets anders dan een computerprogramma. Hilbert's tiende probleem komt dus neer op de vraag of er computerprogramma bestaat waarmee van elke diophantische vergelijking beslist kan worden of het wel of geen oplossing in gehele getallen heeft. Hier is het antwoord,

Stelling 4.1 (Matijasevich, 1970) *Er bestaat geen algoritme (=computerprogramma) om van een willekeurige diophantische vergelijking te beslissen of er wel of geen gehele oplossingen zijn.*

Deze stelling werd in 1970 door Yuri Matijasevich bewezen na belangrijk voorbereidend werk van Martin Davis en Julia Robinson. Hiermee was Hilbert's tiende probleem opgelost, maar misschien niet op de manier die Hilbert bedoeld had.
Het is misschien verrassend dat het mogelijk is de onmogelijkheid van het bestaan van een algoritme aan te tonen. Zoiets was echter niet geheel nieuw, het was al eerder vertoond. In de dertiger jaren van de 20e eeuw is er veel fundamenteel werk binnen de grondslagen van de wiskunde verricht, onder anderen door Turing, Church en Gödel, waarin ook al onbeslisbare problemen werden ontdekt, waaronder het bekende 'Halting probleem'. Een spectaculair resultaat uit die tijd was Gödel's onvolledigheidsstelling die grofweg zegt dat er binnen elk axiomasysteem uitspraken zijn die noch te bewijzen, noch te weerleggen zijn. De stelling van Matijasevich past geheel in deze trend, zij het aan de late kant omdat er eerst nog een aantal lastige problemen uit de weg moesten worden geruimd. Uit het werk van Matijasevich volgt nog meer.

Stelling 4.2 *Er is een polynoom $U(n, x_1, \ldots, x_r)$, dat expliciet geconstrueerd kan worden, met de volgende eigenschap: er bestaat geen enkel algoritme dat voor elke gehele waarde van n kan beslissen of $U(n, x_1, \ldots, x_r) = 0$ oplosbaar is in gehele $x_1, \ldots, x_r$ of niet.*

Er zijn artikelen waarin $U(n, x_1, \ldots, x_r)$ expliciet gegeven wordt. Het zijn reusachtige polynomen, met veel variabelen, die we hier niet zullen reproduceren.
De filosofische impact van Matijasevich's stelling is groot. Allereerst leert het ons dat elke nieuwe diophantische vergelijking een nieuwe uitdaging vormt, er bestaat geen universele methode om ze op te lossen. Een tweede belangrijke consequentie ligt in het volgende. Het blijkt dat veel bekende wiskundige problemen, al of niet opgelost, kunnen worden omgevormd tot een diophantische

vergelijking waarvan aangetoond moet worden dat er geen oplossing bestaat. Voorbeelden van dergelijke problemen zijn:

1. Het Goldbach vermoeden, nog steeds onopgelost, dat zegt dat elk even getal ≥ 4 de som is van twee priemgetallen.

2. De Riemann hypothese, nog steeds onopgelost.

3. De Fermatvergelijking $x^n + y^n = z^n$ in de onbekenden $x, y, z \geq 1$ en $n \geq 3$. Inmiddels opgelost.

4. Het vierkleurenprobleem, inmiddels opgelost.

De diophantische vergelijking die bij elk van deze problemen hoort is gigantisch, ze bevatten tientallen variabelen of hebben een enorm hoge graad. Oplossing van dergelijke vergelijkingen is uitgesloten. Dat neemt echter niet weg dat we hiermee zien dat diophantische vergelijkingen een fundamentelere rol in de wiskunde spelen dan alleen maar als bron van interessante vraagstukken. De stelling van Matijasevich laat zien dat we de oplossing van diophantische vergelijkingen, het bewijs van bijvoorbeeld het Goldbach probleem en de Riemann hypothese niet kunnen overlaten aan een machine. Het aangaan van deze uitdagingen blijft mensenwerk.

Chaos, voorspelbaarheid, en bemonstering

Jason Frank
Centrum Wiskunde & Informatica
e-mail: J.E.Frank@cwi.nl

In dit college behandelen we lange-tijd simulaties van chaotische dynamische systemen, met als doel de bemonstering van zulke systemen voor statistische analyse. We onderzoeken de mate waarin men nog kan spreken van voorspelbaarheid van dergelijke systemen. Onze primaire motivatie is weers- en klimaatvoorspelling, maar de begrippen worden geïllustreerd aan de hand van simpele voorbeelden uit ook andere toepassingsgebieden.

1 Differentievergelijkingen

Voorspellingsproblemen worden doorgaans omschreven als dynamische systemen. De belangrijkste ingrediënten zijn een variabele die de toestand van het systeem beschrijft op een gegeven tijdstip, en een voorschrift voor het propageren van de toestand op één tijdstip naar de volgende.

Bijvoorbeeld, in het logistieke model voor bevolkingsgroei (met beperkte capaciteit), is de oorspronkelijke populatie aangeduid met P_0. Het voorschrift voor het propageren van de oplossing is

$$P_{n+1} = P_n + \Delta t\, R\, P_n(1 - P_n) \tag{1}$$

waarbij $R > 0$ een parameter is die de snelheid van de bevolkingsgroei bepaalt en P_n uitgedrukt wordt als een percentage van de maximale populatie. Duidelijk is dat, gegeven P_0, we deze formule kunnen gebruiken (met $n = 0$) om P_1 te berekenen, en dat gegeven P_1 de formule (met $n = 1$) P_2 geeft, enzovoort. Deze recursie genereert een reeks

$$P_0, P_1, P_2, \ldots$$

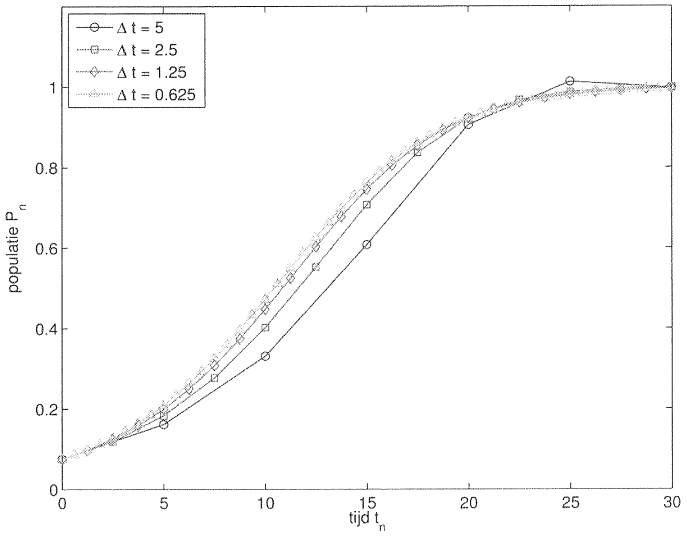
waarvan we hopen dat het de omvang van de bevolking weergeeft op de tijdstippen

$$t_0, t_1, t_2, \ldots$$

waarbij $t_{n+1} = t_n + \Delta t$. Met andere woorden, we willen dat P_n een betrouwbare schatting is van de exacte omvang (als percentage) van de maximale populatie. Een voorschrift als (1) voor het propageren van de oplossing van tijdstip t_n naar tijdstip t_{n+1} wordt een *differentievergelijking* genoemd.

Beschouw vervolgens een interval, $t \in [0, T]$, waarin we de oplossing willen weten. We verdelen het interval in N stappen van grootte $\Delta t = T/N$ en passen (1) N keer toe om een reeks te genereren. We kunnen een grafiek maken van de punten (t_n, P_n) om de bevolkingsgroei te visualiseren (zie Figuur 1). Vervolgens nemen we $\Delta t = T/(2N)$ en nemen nu $2N$ stappen om een tweede reeks te

genereren. Wij zetten de punten (t_n, P_n) van deze nieuwe reeks in dezelfde grafiek. Als we dit proces herhalen, elke keer het aantal stappen verdubbelen, en tegelijk de stapgrootte halveren, en elke keer de reeks uitzetten in de grafiek, constateren we dat de resultaten uiteindelijk niet te onderscheiden zijn — het proces convergeert naar een continue functie.



Figuur 1: Convergentie van het logistieke model voor steeds kleinere tijdstappen.

Meestal is meer dan één variabele nodig om de toestand van een systeem weer te geven. Bijvoorbeeld, de toestand van een slinger in het vlak wordt bepaald door de hoek θ ten opzichte van de zwaartekrachtsrichting en de hoeksnelheid v. Een geschikte differentievergelijking voor een slinger van lengte ℓ met zwaartekracht parameter g is:

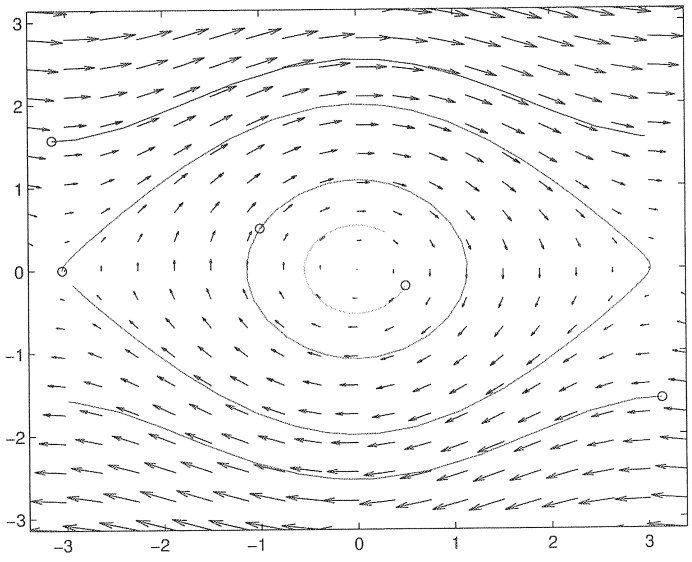
$$\theta_{n+1} = \theta_n + \Delta t\, v_n \tag{2}$$

$$v_{n+1} = v_n - \Delta t\, \frac{g}{\ell} \sin \theta_{n+1}. \tag{3}$$

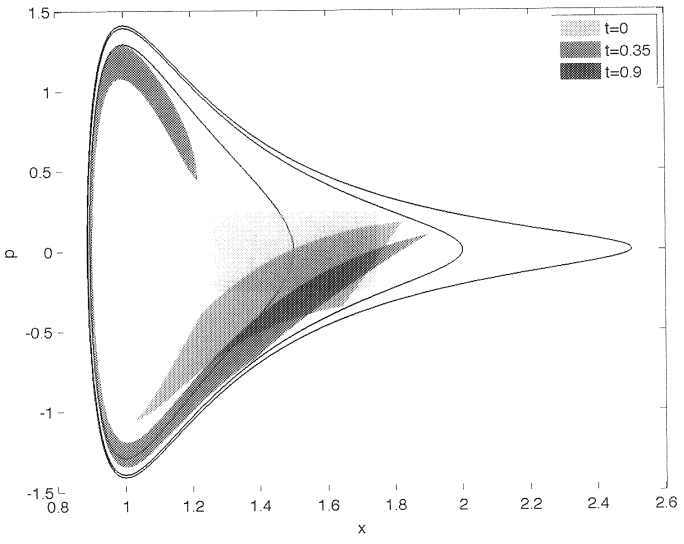
We kunnen de grafiek van de reeksen (t_n, θ_n) en (t_n, v_n) apart uitzetten als tijdsreeksen. Maar we kunnen ook de punten (θ_n, v_n) beschouwen als coördinaten in de ruimte van de toestandsvariabelen die het systeem beschrijven, dat wil zeggen de *faseruimte*. Elk punt (θ, v) in de faseruimte definieert een mogelijke toestand van het systeem. De reeks punten die gegenereerd worden via de differentievergelijkingen (2)–(3), markeren een pad of traject in de faseruimte.

Als we van een andere begintoestand (θ_0, v_0) beginnen, krijgen we een andere traject in de faseruimte. Door een aantal karakteristieke oplossingen uit te zetten krijgen we een beeld van de structuur van de faseruimte (zie Figuur 2). Soms zijn we geïnteresseerd in een hele verzameling van beginvoorwaarden. Bijvoorbeeld, soms weten we de exacte begintoestand niet, maar weten we alleen een kansverdeling op een bepaalde verzameling van mogelijke begintoestanden. Een verzameling van oplossingstrajecten wordt een *ensemble* genoemd. Een

continue verzameling van begintoestanden zal meestal worden vervormd als het ensemble evolueert (zie Figuur 3).



Figuur 2: Een aantal trajecten in de faseruimte van de slinger. De begintoestanden worden aangeduid met een cirkel.



Figuur 3: Evolutie van een ensemble.

2 Voorspelbaarheid

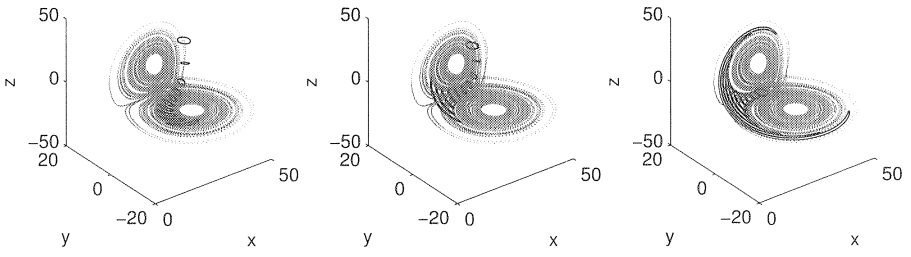
Sommige modellen zijn vergevingsgezind. Een kleine fout in de begintoestand zal uiteindelijk verdwijnen, en oplossingen die in de buurt van elkaar liggen convergeren naar elkaar. Dit is echter eerder uitzondering dan regel. Complexe niet-lineaire systemen vertonen meestal een zekere mate van *chaos* - nabijgelegen trajecten divergeren exponentieel.

Het meest bekende voorbeeld van een chaotisch systeem is wellicht het systeem dat voorgesteld werd door E.N. Lorenz in 1963 [2]. Het Lorenz-systeem, geschreven in de vorm van een differentievergelijking in de drie variabelen x_n, y_n en z_n, luidt

$$x_{n+1} = x_n + \Delta t\,(-\beta x_n + y_n z_n) \tag{4}$$
$$y_{n+1} = y_n + \Delta t\,(-\sigma y_n + \sigma z_n) \tag{5}$$
$$z_{n+1} = z_n + \Delta t\,(-x_n y_n + \rho y_n - z_n) \tag{6}$$

waarbij $\beta = 8/3$, $\sigma = 10$ en $\rho = 28$.

Om te zien hoe nabijgelegen oplossingen divergeren, beschouwen we ensemble simulaties, zoals weergegeven in Figuur 4. Deze afbeelding is geleend van [3]. Een verzameling van 1000 begintoestanden worden geselecteerd, die oorspronkelijk op een cirkel in de faseruimte liggen. Voor elk van deze toestanden, worden er 100 stappen van de differentievergelijking (4)–(6) uitgevoerd, met tijdstap $\Delta t = 0.06$. De oplossingen worden uitgezet in Figuur 4 op een achtergrond van een enkel, zeer lang traject, die de Lorenz attractor weergeeft. Ensemble simulaties kunnen worden uitgevoerd voor een grote, maar eindige verzameling van nabijgelegen beginwaarden, om de voorspelbaarheid van het probleem te onderzoeken. Afhankelijk van waar in de faseruimte de trajecten afkomstig zijn, blijven ze ofwel in de buurt van elkaar of hebben ze de neiging af te wijken, mogelijk sterk. Echte weersvoorspelling is vergelijkbaar. Relatief stabiele weerpatronen zijn veel beter te voorspellen dan onstabiele.

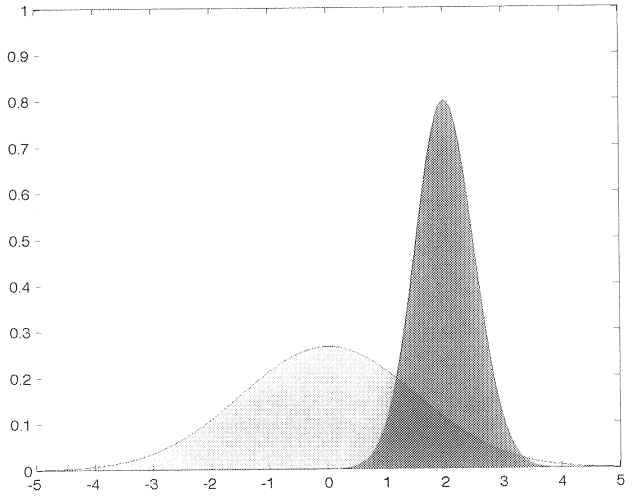


Figuur 4: Ensemble simulaties met het Lorenz-model illustreren dat sommige begintoestanden betere voorspelbaarheid hebben dan anderen. Het licht grijze traject weergeeft de Lorenz Attractor, de zwarte punten zijn de ensemble trajecten.

Ensemble simulaties vormen een nuttige instrument voor het schatten van de waarschijnlijkheid van verschillende weerscenario's. Uitgaande van de huidige toestand van de atmosfeer, worden een groot aantal simulaties gedraaid, elk

vanuit een iets verstoorde begintoestand. Hieruit kan men bepalen met behulp van statistische analyses wat de meest waarschijnlijke uitkomsten zijn (bv. "een 70% kans op regen"). Ook minder waarschijnlijke, maar potentieel gevaarlijke, scenario's kunnen worden berekend (bv. "een 1% kans op noodweer").

Het doel van ensemble simulaties is om een kansdichtheidsfunctie te bepalen voor de waarschijnlijkheid van een specifieke gebeurtenis. De mate waarin een bepaalde simulatie ons daadwerkelijk nieuwe informatie geeft wordt aangeduid als de *voorspellende kracht* van de simulatie. Uit één zeer lange simulatie is het mogelijk een kansverdeling te bepalen die onafhankelijk is van de begintoestand. Dit is de klimatologisch-gemiddelde distributie, geïllustreerd door het licht grijze gebied in Figuur 5. De voorspellende kracht van een ensemble simulatie is de mate waarin een voorspelde ensemble (donker grijs gebied) verschilt van de klimatologische gemiddelde. Voor meer informatie hierover, zie [3].



Figuur 5: Waarschijnlijkheidsdichtheid van een bepaalde voorspelling (donker grijs) vergeleken met de klimatologische gemiddelde verdeling (licht grijs). Een dergelijke verdeling heeft voorspellende kracht.

3 Rol van het model

De differentievergelijkingen die gebruikt worden in de voorbeelden hierboven zijn niet uniek. Bijvoorbeeld, een alternatief model voor de slinger is

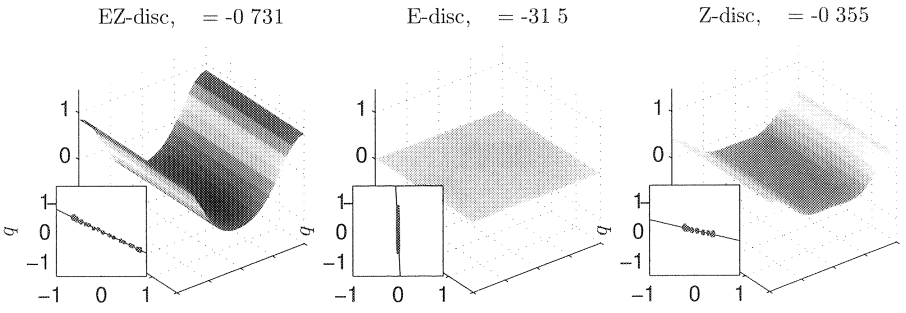
$$\theta_{n+1} = \theta_n + \Delta t\, v_n \tag{7}$$

$$v_{n+1} = v_n - \Delta t\, \frac{g}{\ell} \sin\theta_n. \tag{8}$$

Het enige verschil is dat in dit geval $\sin\theta$ wordt geëvalueerd op tijdstip n in de tweede vergelijking. Hoewel beide modellen convergeren naar dezelfde continue functie voor Δt naar nul op een vast interval $[0, T]$, geven ze zeer verschillend gedrag voor vaste Δt wanneer een simulatie wordt gedraaid door vele oscillaties

van de slinger. In het bijzonder lijkt het model (2)–(3) de periodieke beweging van de slinger goed weer te geven, terwijl de oscillaties van het nieuwe model een monotoon stijgende amplitude tonen. Het is duidelijk dat wanneer men geïnteresseerd is in het berekenen van statistische gemiddelden, het model met toenemende amplitude statistisch vertekende resultaten zal weergeven. Het cruciale verschil tussen de modellen is het behoud van energie door de eerste.

Vergelijkbaar gedrag kan worden gezien in de modellen die worden gebruikt voor weer- en klimaatsimulaties. Als voorbeeld, Figuur 6 toont het resultaat van lange simulaties met drie verschillende modellen voor een windstroming over topografie. De vlakken in de Figuur illustreren de gemiddelde windvelden in een vallei. De steilheid van het oppervlak representeert de relatieve sterkte van het windveld, dat waait langs contourlijnen van de getoonde oppervlakken. Het actuele windveld op elk moment t_n is meestal vrij complex, maar door te middelen over lange tijd wordt dit gladgestreken. Het meest opvallende van het figuur is dat de drie verschillende methoden (differentievergelijkingen) die gebruikt zijn, heel andere voorspellingen voor de heersende wind geven. In het eerste geval zijn de gemiddelde winden vrij sterk, zoals aangeduid door de steile trog. In het tweede geval, is de gemiddelde toestand windstil, en in het laatste geval matig. De verschillen in de methoden zijn te wijten aan hun verschillende behoud van fysische wetten. Huidig onderzoek richt zich op de betrouwbaarheid van numerieke simulaties voor statistische voorspelling en de constructie van statistisch nauwkeurige modellen [1].



Figuur 6: Niveau van de gemiddelde windsnelheid in een vereenvoudigd atmosferisch model, berekend op basis van drie verschillende methoden.

Referenties

[1] S. Dubinkina & J. Frank, "Statistical mechanics of Arakawa's discretizations", *Journal of Computational Physics* **227** (2007) 1286–1305.

[2] E. N. Lorenz, "Deterministic non-periodic flow", *Journal of the Atmospheric Sciences* **20** (1963) 130–148.

[3] T. N. Palmer, F. J. Doblas-Reyes, R. Hagedorn & A. Weisheimer, "Probabilistic prediction of climate using multi-model ensembles: from basics to applications", *Philosophical Transactions of the Royal Society B* **360** (2005) 1991–1998.

Verrassende wiskunde bij de Olympiade

Quitijn Puite
Technische Universiteit Eindhoven en
Hogeschool Utrecht
e-mail: g.w.q.puite@tue.nl
http://www.win.tue.nl/~gpuite

1 Inleiding

Elk schooljaar doen er 30 leerlingen mee aan de landelijke training voor de Internationale Wiskunde Olympiade, die elke zomer in een ander land plaats vindt. Tijdens deze training, die loopt van half november tot half juni, krijgen de leerlingen veel nieuwe theorie te zien: van modulorekenen en de kleine stelling van Fermat tot de concurrentiestelling van Ceva. De volgende opgave is bijvoorbeeld goed op te lossen door handig te modulorekenen:

Opgave Bepaal alle paren (x, y) van gehele getallen die voldoen aan

$$5x^2 - 3y^2 = 2011.$$

Uitwerking Het blijkt handig te zijn om modulo 4 te rekenen. Het kwadraat van een even getal, zeg $2k$, is $(2k)^2 = 4k^2$, dus dat is 0 modulo 4. Het kwadraat van een oneven getal, zeg $2k + 1$, is $4k^2 + 4k + 1$, dus dat is 1 modulo 4. Kwadraten zijn dus altijd 0 of 1 modulo 4.
Stel nou eens dat (x, y) een oplossing is. Dan geldt dus $5x^2 - 3y^2 = 2011$. Door er $4y^2 - 4x^2$ bij op te tellen, zien we dat de linkerkant op een veelvoud van 4 na gelijk is aan $x^2 + y^2$.
Nu is de som van twee kwadraten modulo 4 gelijk aan $0 + 0$ of $0 + 1$ of $1 + 1$. Maar 2011 is echter gelijk aan 3 modulo 4. Dit geeft een tegenspraak. Er zijn dus geen oplossingen. □

Behalve deze 'hogere wiskunde', komen ook elementaire bewijsprincipes ruimschoots bij de olympiadetraining aan bod. In de lezing staat een aantal van zulke 'gezond-verstand-technieken' centraal. Aan de orde komen problemen oplossen met behulp van het ladenprincipe, kleuringen, invariantie en het extremenprincipe.

Daarmee is het mogelijk om van elk van de volgende opgaven een even simpele als geniale oplossing te geven.

1. Van 16 tot 24 juli 2011 vindt in Nederland de Internationale Wiskunde Olympiade plaats.
   Bewijs dat er een veelvoud van 2011 is dat alleen maar uit enen bestaat (in decimale notatie). (Zie opgave 6.)

2. In een rij van tien bomen zitten tien spreeuwen, in elke boom één. Op het moment dat een spreeuw een willekeurig aantal k bomen naar rechts vliegt, vliegt een andere spreeuw k bomen naar links.
   Kunnen alle spreeuwen uiteindelijk in één boom terecht komen? (Zie opgave 15.)

3. Gegeven zijn $2n$ punten in het vlak, geen drie hiervan op één lijn. De helft van deze punten stelt boerderijen voor, de andere helft waterputten. Bewijs dat het mogelijk is om elke boerderij door middel van een kaarsrechte weg zodanig met een unieke waterput te verbinden, dat al deze n verbindingswegen elkaar niet snijden. (Zie opgave 20.)

Bronvermelding

De opgaven zijn een selectie uit het olympiadetrainingsmateriaal dat in de loop der tijd door de trainers van de wiskundeolympiade is samengesteld. Een groot aantal opgaven staat ook in *Arthur Engel,* Problem-Solving Strategies.

www.imo2011.nl
www.wiskundeolympiade.nl
www.win.tue.nl/~gpuite/lesbrief/

2 Ladenprincipe

Het ladenprincipe zegt:

> Als je meer dan n balletjes over n laatjes verdeelt, dan is er ten minste één laatje dat meer dan één balletje bevat.

Of, wat algemener:

> Als je meer dan kn balletjes verdeelt over n laatjes, dan is er ten minste één laatje waar meer dan k balletjes in zitten.

Het bewijs van dit principe gaat uit het ongerijmde. Uitgaande van de meer dan kn balletjes die zijn verdeeld over n laatjes, stel dat het niet zo is dat er ten minste één laatje is waar meer dan k balletjes in zitten. Dan zitten in alle laatjes dus ten hoogste k balletjes. Het totale aantal balletjes is dan ten hoogste $n \cdot k$. Maar dat is in tegenspraak met het aantal van meer dan kn verdeelde balletjes.

Ook al is dit principe zelf nogal eenvoudig, je kunt het soms op een zeer verrassende manier inzetten om ingewikkelde opgaven op te lossen. Daarbij is het de kunst om geschikte laatjes en balletjes te vinden. En vervolgens om de juiste conclusie te trekken uit het feit dat er $k + 1$ balletjes in één en hetzelfde laatje zitten.

Voorbeeld

Opgave In een kubusvormig aquarium met zijden van 17 meter zwemmen 10 000 vissen. Bewijs dat er op elk moment een kubus met zijden van 1 meter in het aquarium te vinden is waarin minstens drie vissen zwemmen. (We beschouwen de vissen als punten. Een vis kan dus niet gedeeltelijk in een gegeven kubus en gedeeltelijk daarbuiten zwemmen.)

Uitwerking We bekijken een willekeurig moment en bevriezen even de positie van de vissen op dat moment. Verder delen we het aquarium in 17^3 kubussen met zijden van 1 meter; dit worden onze laatjes. Voor elke kubus doen we een balletje in het bijbehorende laatje voor elke vis die in deze kubus zwemt. Als een vis op de grens van twee of meer kubussen zwemt, komen er voor deze vis meerdere balletjes in meerdere laatjes (maar slechts één per laatje). Op deze manier stoppen we ten minste 10 000 balletjes in $17^3 = 4913$ laatjes. Omdat $10\,000 > 2 \cdot 4913$, volgt met het ladenprincipe hieruit dat er een kubus is waar op dit moment ten minste drie vissen in zwemmen. □

Opgaven

Opgave 1 *Gegeven is een vierkant $ABCD$ met lengte der zijden gelijk aan 1. Laat verder vijf punten P_1, P_2, P_3, P_4 en P_5 gegeven zijn in het inwendige van het vierkant of op de rand. Noem d_{ij} de afstand tussen P_i en P_j.*
Bewijs dat ten minste één van deze afstanden d_{ij} niet groter is dan $\frac{1}{2}\sqrt{2}$.

Opgave 2 *Gegeven is een verzameling A van 20 verschillende gehele getallen uit de rekenkundige rij*

$$1, 4, 7, \ldots, 97, 100.$$

Bewijs dat A een tweetal elementen bevat met som 104.

Opgave 3 *In een restaurant zitten $n \geq 2$ mensen aan een ronde tafel. Iedereen heeft een ander gerecht besteld. De ober zet alle bestelde gerechten op tafel, één voor elke persoon. Echter, hij doet dit zo dat geen enkel gerecht bij de juiste persoon staat.*
Bewijs dat het mogelijk is om de tafel zodanig te draaien dat ten minste twee mensen het juiste gerecht voor hun neus hebben.

Opgave 4 *We hebben gegeven een getal N bestaande uit 16 cijfers. Bewijs dat je een aantal achtereenvolgende cijfers van N met elkaar kunt vermenigvuldigen zodat het resultaat een kwadraat van een geheel getal is.*

Opgave 5 ***(IMO1972, opgave 1)*** *De verzameling U bevat 10 verschillende gehele getallen tussen de 1 en de 100 (inclusief). Bewijs dat er twee disjuncte niet-lege deelverzamelingen van U zijn met gelijke som van de elementen.*
Voorbeeld: $U = \{2, 7, 13, 35, 41, 59, 63, 72, 81, 95\}$; dan bijv. $2+7+13+41 = 63$ of $7 + 41 = 13 + 35$.

Opgave 6 ***(Zie inleiding, opgave 1)*** *Gegeven is een positief geheel getal n dat niet deelbaar is door 2 of 5. Bewijs dat er een veelvoud van n is dat alleen maar uit enen bestaat (in decimale notatie).*

Opgave 7 *De verzameling S bevat $n + 1$ verschillende getallen uit*

$$\{1, 2, \ldots, 2n\}.$$

Bewijs dat er twee getallen a en b in S te vinden zijn zodat $a \mid b$.

3 Kleuringen

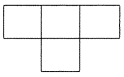
Gegeven een bord van een bepaalde vorm en puzzelstukjes (of dominosteentjes) van een bepaalde vorm. We kunnen ons dan afvragen of het mogelijk is om met de gegeven stukjes het bord te overdekken. Als we willen bewijzen dat dit niet kan, is het soms handig om het bord op een bepaalde manier te kleuren.

Voorbeeld

Opgave Bekijk een 8×8-bord waarvan twee schuin tegenover elkaar liggende hoekjes weg zijn. Kun je de 62 overgebleven vakjes bedekken met 2×1-stenen?

Uitwerking Kleur de vakjes om en om zwart en wit als op een schaakbord. De hoekjes die weg zijn, zouden allebei dezelfde kleur gekregen hebben. Er zijn dus nu 30 vakjes van de ene kleur en 32 van de andere. Elke 2×1-steen bedekt precies één vakje van elke kleur. Het is dus onmogelijk om met deze stenen 30 vakjes van de ene en 32 vakjes van de andere kleur te bedekken. Dus we kunnen het bord niet bedekken met deze stenen. □

Opgaven



Figuur 1: Een T-tetromino.

Opgave 8 *Bewijs dat een* 10×10*-bord niet bedekt kan worden door 25 T-tetromino's.*

Opgave 9 *Midden in een* $3 \times 3 \times 3$*-kubus van kaas zit een muis. Hij heeft het middelste blokje kaas al opgegeten. De muis wil zich een weg eten door de kubus van kaas door steeds naar aangrenzende blokjes kaas te gaan en deze op te eten. Hij mag dus niet langs een blokje dat hij al eerder opgegeten heeft en hij mag niet buiten de kubus komen. Kan hij alle blokjes kaas opeten?*

Opgave 10 *Is het mogelijk een rechthoek van* 16×9 *vakjes te onderverdelen in 24 stenen van* 1×6*? (uit* Mijn Mooiste Mathe *van Leon van den Broek)*

Opgave 11 *Laat zien dat je een* 10×10*-bord niet kunt bedekken met* 1×4*-stenen.*

Opgave 12 *Hoeveel bakstenen van 1 bij 1 bij 4 passen in een kubusvormige doos met zijde 6?*

Opgave 13 *Een rechthoekige vloer is bedekt met een combinatie van* 1×4*- en* 2×2*-tegels. Als we één tegel vervangen door een tegel van de andere soort, kunnen we dan nog steeds de vloer bedekken?*

4 Invariantie

Het principe van invariantie kun je gebruiken bij opgaven waar je gegeven hebt:

- een beginsituatie,
- een eindsituatie,
- een of meer toegestane stappen.

De vraag is dan vaak: kun je vanuit de beginsituatie de eindsituatie bereiken door alleen toegestane stappen te doen? Als je vermoedt dat dit niet mogelijk is, kun je dit proberen te bewijzen met behulp van invariantie. Hierbij zoek je een waarde die bij het doen van een toegestane stap niet verandert, een zogeheten *invariant*. Als deze waarde in de begin- en eindsituatie niet hetzelfde is, dan is het onmogelijk om vanuit de beginsituatie de eindsituatie te bereiken.

Voorbeeld

Opgave Beginnend met een rij van vijf enen en zes nullen mag je telkens twee getallen wegstrepen en er één voor in de plaats zetten. Als je twee dezelfde getallen wegstreept, zet je een nul ervoor terug. Als je twee verschillende getallen wegstreept, zet je een één ervoor terug. Eindig je altijd met hetzelfde getal?

Uitwerking Definieer S als de som van de getallen in de rij. Wat gebeurt er nu met S als je twee cijfers wegstreept?

- Als je twee enen wegstreept, dan komt er een nul voor in de plaats en wordt S dus twee kleiner.
- Als je twee nullen wegstreept, dan komt er een nul voor in de plaats en blijft S gelijk.
- Als je een één en een nul wegstreept, dan komt er een één voor in de plaats en blijft S gelijk.

We concluderen dat bij de toegestane stappen de pariteit van S niet verandert. In de beginsituatie is $S = 5$. In de eindsituatie staat er nog precies één getal op het bord. Dit getal moet dus oneven zijn, omdat S oneven moet zijn. Dus dit getal kan alleen een één zijn. □

Opgaven

Opgave 14 *Op een 8×8-schaakbord zijn alle vakjes wit gekleurd op één zwart vakje na. Je mag elke rij en elke kolom herkleuren, d.w.z. elk vakje in zo'n rij of kolom wordt wit als het zwart was en zwart als het wit was. Kun je alle vakjes wit krijgen?*

Opgave 15 ***(Zie inleiding, opgave 2)*** *In een rij van tien bomen zitten tien spreeuwen, in elke boom één. Op het moment dat een spreeuw een willekeurig aantal k bomen naar rechts vliegt, vliegt een andere spreeuw k bomen naar links. Kunnen alle spreeuwen uiteindelijk in één boom terecht komen?*

Opgave 16 *Op een eiland wonen 13 grijze, 15 bruine en 17 rode kameleons. Als twee kameleons met verschillende kleuren elkaar tegenkomen, veranderen ze hun kleur in de derde kleur. Kunnen op een gegeven moment alle kameleons dezelfde kleur hebben?*

Opgave 17 *De getallen 1, 2, ..., 20 staan op een krijtbord. We mogen twee willekeurige getallen a en b vervangen door het getal $ab + a + b$. Welk getal blijft er over nadat je dit 19 keer gedaan hebt?*

Opgave 18 *Van een $n \times n$-bord is een aantal vakjes ziek. Deze ziekte is erg besmettelijk. Als een vakje minstens twee zijden gemeen heeft met zieke vakjes, dan wordt dat vakje zelf ook ziek. Aan het eind van de epidemie blijkt elk vakje van het bord ziek te zijn. Hoeveel vakjes waren er aan het begin minstens ziek?*

5 Extremenprincipe

Gegeven een verzameling objecten kan het nuttig zijn om naar het kleinste of grootste object te kijken. Dat is het idee van het extremenprincipe. Het kleinste of grootste object heeft vaak speciale eigenschappen die de andere objecten in de verzameling niet hebben en daar kun je handig gebruik van maken.

Let op! Niet elke verzameling heeft een kleinste of grootste element. Je moet dit altijd controleren voordat je het extremenprincipe toe gaat passen. Je kunt hiervoor de volgende principes gebruiken.

1. Elke niet-lege *eindige* deelverzameling van de reële getallen heeft een minimum en een maximum.
2. Elke niet-lege deelverzameling van de *natuurlijke* getallen heeft een minimum.

Voorbeeld

Opgave Een eindig aantal steden is verbonden door een aantal éénrichtingsverkeerwegen. Voor elk tweetal steden A en B is het mogelijk om via deze wegen van A naar B te komen of van B naar A te komen. Bewijs dat er een stad is die vanuit elke andere stad bereikbaar is.

Uitwerking Tel voor elke stad het aantal andere steden waarvandaan deze stad bereikbaar is. Zij M het maximum van deze aantallen (dat bestaat op grond van principe 1) en zij A een stad die vanuit M andere steden bereikbaar is. Als A vanuit alle andere steden bereikbaar is, zijn we klaar. Zo niet, dan is er een stad B waarvandaan A niet bereikbaar is. Maar dan is B wel vanuit A bereikbaar. Van elk van de M steden waarvandaan A bereikbaar is, kun je nu ook B bereiken: eerst naar A en vervolgens over de route van A naar B. Ook vanuit A kun je B bereiken, dus B is te bereiken vanuit minstens $M+1$ steden. Tegenspraak, want M was maximaal. Dus A is vanuit alle andere steden bereikbaar. □

Opgaven

Opgave 19 *Elk roosterpunt $(x, y) \in \mathbb{Z}^2$ wordt gelabeld met een positief geheel getal, en wel zodanig dat voor elk punt z'n label het gemiddelde is van de labels van z'n vier buren. Bewijs dat alle labels gelijk zijn.*

Opgave 20 ***(Zie inleiding, opgave 3)*** *Gegeven zijn $2n$ punten in het vlak, geen drie hiervan op één lijn. De helft van deze punten stelt boerderijen voor, de andere helft waterputten. Bewijs dat het mogelijk is om elke boerderij door middel van een kaarsrechte weg zodanig met een unieke waterput te verbinden, dat al deze n verbindingswegen elkaar niet snijden.*

Opgave 21 *Gegeven is een eindige verzameling V van punten in het vlak zodanig dat elke lijn die door twee punten van V gaat, ook door een derde gaat. Bewijs dat alle punten op één lijn liggen.*
(Equivalent) Zij gegeven een eindige verzameling V van punten in het vlak zodanig dat ze niet allemaal op één lijn liggen. Bewijs dat er een lijn is die door precies twee punten van V gaat.

6 Uitwerkingen

Opgave 1 *Gegeven is een vierkant $ABCD$ met lengte der zijden gelijk aan 1. Laat verder vijf punten P_1, P_2, P_3, P_4 en P_5 gegeven zijn in het inwendige van het vierkant of op de rand. Noem d_{ij} de afstand tussen P_i en P_j.*
Bewijs dat ten minste één van deze afstanden d_{ij} niet groter is dan $\frac{1}{2}\sqrt{2}$.

Uitwerking Deel het vierkant op in vier even grote $\frac{1}{2} \times \frac{1}{2}$-vierkantjes. Eén van deze vierkantjes bevat volgens het ladenprincipe ten minste twee van de vijf punten, zeg P_1 en P_2. De afstand tussen P_1 en P_2 is dus niet groter dan de maximale afstand in dit $\frac{1}{2} \times \frac{1}{2}$-vierkantje, en dat is $\frac{1}{2}\sqrt{2}$. □

Opgave 2 *Gegeven is een verzameling A van 20 verschillende gehele getallen uit de rekenkundige rij*

$$1, 4, 7, \ldots, 97, 100.$$

Bewijs dat A een tweetal elementen bevat met som 104.

Uitwerking Bekijk de 18 laatjes $\{1\}$, $\{4, 100\}$, $\{7, 97\}$, $\{10, 94\}$, $\{13, 91\}$, $\{16, 88\}$, $\{19, 85\}$, $\{22, 82\}$, $\{25, 79\}$, $\{28, 76\}$, $\{31, 73\}$, $\{34, 70\}$, $\{37, 67\}$, $\{40, 64\}$, $\{43, 61\}$, $\{46, 58\}$, $\{49, 55\}$, $\{52\}$. Als we daar $20 > 18$ verschillende getallen over verdelen, dan moet wel ten minste één laatje dubbel worden gevuld. Per constructie van de laatjes, hebben we dan een tweetal elementen met som 104. □

Opgave 3 *In een restaurant zitten $n \geq 2$ mensen aan een ronde tafel. Iedereen heeft een ander gerecht besteld. De ober zet alle bestelde gerechten op tafel, één voor elke persoon. Echter, hij doet dit zo dat geen enkel gerecht bij de juiste persoon staat.*
Bewijs dat het mogelijk is om de tafel zodanig te draaien dat ten minste twee mensen het juiste gerecht voor hun neus hebben.

Uitwerking Maak de laatjes "na $1\times$ draaien op de goede plek" t/m "na $(n-1)\times$ draaien op de goede plek". Daar worden de $n > n-1$ gerechten over verdeeld, afhankelijk van na hoeveel keer draaien het gerecht op de goede plek staat. Volgens het ladenprincipe is ten minste één van deze laatjes, zeg "na $k\times$ draaien op de goede plek", met twee of meer gerechten gevuld. Maar dat wil zeggen dat na k keer draaien ten minste twee mensen het juiste gerecht voor hun neus hebben. □

Opgave 4 *We hebben gegeven een getal N bestaande uit 16 cijfers. Bewijs dat je een aantal achtereenvolgende cijfers van N met elkaar kunt vermenigvuldigen zodat het resultaat een kwadraat van een geheel getal is.*

Uitwerking Als er een nul voorkomt onder de 16 cijfers, is het resultaat duidelijk (want 0 is een kwadraat). Stel nu dat alle cijfers ongelijk 0 zijn. Schrijf $N = \overline{a_1 a_2 \ldots a_{16}}$ en bekijk de priemfactorontbinding van $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ voor $k = 0$ t/m 16. (Voor $k = 0$ staat hier het lege product; dat is 1.) We gaan voor elke k kijken of priemfactor 2 een even of een oneven aantal keer voorkomt in $a_1 \cdot a_2 \cdot \ldots \cdot a_k$, en hetzelfde voor priemfactoren 3, 5 en 7. Meer priemfactoren komen er niet voor in $a_1 \cdot a_2 \cdot \ldots \cdot a_k$.
Qua pariteit van het aantal priemfactoren 2, 3, 5 en 7 in $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ zijn er $2 \times 2 \times 2 \times 2 = 16$ mogelijkheden. Dus er zijn twee k'tjes (zeg $k = k_1$ en $k = k_2$ met $k_1 < k_2$) waarvoor in de uitdrukkingen $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ priemfactor 2 beide keren even of juist beide keren oneven voor komt, en idem voor 3, 5, 7. Derhalve is het quotiënt $a_1 \cdot a_2 \cdot \ldots \cdot a_{k_2}$ gedeeld door $a_1 \cdot a_2 \cdot \ldots \cdot a_{k_1}$ een kwadraat, want alle priemfactoren zitten hier een even aantal keer in. Dit quotiënt is precies $a_{k_1+1} \cdot a_2 \cdot \ldots \cdot a_{k_2}$. □

Opgave 5 ***(IMO1972, opgave 1)*** *De verzameling U bevat 10 verschillende gehele getallen tussen de 1 en de 100 (inclusief). Bewijs dat er twee disjuncte niet-lege deelverzamelingen van U zijn met gelijke som van de elementen.*
Voorbeeld: $U = \{2, 7, 13, 35, 41, 59, 63, 72, 81, 95\}$; dan bijv. $2+7+13+41 = 63$ *of* $7 + 41 = 13 + 35$.

Uitwerking Er zijn $2^{10} - 1 = 1023$ niet-lege deelverzamelingen D, variërend van $D = \{x\}$ (met "som" minstens 1) tot $D = U$ (met som hooguit $91 + 92 + \cdots + 100 = \frac{1}{2} \cdot 10 \cdot 191 = 955$). Voor de 1023 niet-lege deelverzamelingen zijn er dus 955 mogelijkheden voor hun som, dus zijn er twee verschillende deelverzamelingen D_1 en D_2 met gelijke som. Weglaten van de gemeenschappelijke elementen geeft twee verschillende disjuncte deelverzamelingen E_1 en E_2, nog steeds met gelijke som. Als E_1 nu leeg zou zijn, dan is E_2 niet leeg maar heeft hij wel som van de elementen gelijk aan 0; tegenspraak. Dus E_1 (en zo ook E_2) zijn bovendien niet-leeg. Dit zijn dus de gevraagde disjuncte niet-lege deelverzamelingen van U. □

Opgave 6 ***(Zie inleiding, opgave 1)*** *Gegeven is een positief geheel getal n dat niet deelbaar is door 2 of 5. Bewijs dat er een veelvoud van n is dat alleen maar uit enen bestaat (in decimale notatie).*

Uitwerking Bekijk de $n + 1$ getallen $1_1 := 1$, $1_2 := 11$, $1_3 := 111$, ..., $1_{n+1} := \underbrace{11\ldots11}_{n+1 \text{ enen}}$ en kijk naar hun resten bij deling door n. Omdat er maar n resten mogelijk zijn (namelijk $0, 1, \ldots, n-1$), hebben ten minste twee van de genoemde 1_i, zeg 1_p en 1_q met $p > q$, dezelfde rest bij deling door n. Dus hun verschil is een n-voud:

$$1_p - 1_q = 11\ldots1100\ldots00 = 1_{p-q} \cdot 10^q = 1_{p-q} \cdot 2^q \cdot 5^q$$

is een n-voud. Omdat n geen delers 2 en 5 bevat, moet 1_{p-q} ook wel een n-voud zijn. □

Opgave 7 *De verzameling S bevat $n+1$ verschillende getallen uit*

$$\{1, 2, \ldots, 2n\}.$$

Bewijs dat er twee getallen a en b in S te vinden zijn zodat $a \mid b$.

Uitwerking Neem n laden met stickers 1, 3, ..., $2n-1$. Stop elk getal van S in de lade die zijn grootste oneven deler aangeeft. Er is een lade, zeg met sticker m, waarin minstens twee getallen uit S zitten. Deze getallen zijn dan van de vorm $2^i m$ en $2^j m$ met $i < j$ en er geldt $2^i m \mid 2^j m$. □

Opgave 8 *Bewijs dat een 10×10-bord niet bedekt kan worden door 25 T-tetromino's.*

Uitwerking Kleur het bord als een schaakbord. Elke T-tetromino bedekt ofwel drie zwarte en één wit vakje, ofwel drie witte en één zwart vakje. We hebben een oneven aantal tetromino's, dus we kunnen nooit evenveel zwarte als witte vakjes bedekken. Het bord heeft echter wel evenveel zwarte als witte vakjes. Dus de T-tetromino's kunnen niet het bord bedekken. □

Opgave 9 *Midden in een $3 \times 3 \times 3$-kubus van kaas zit een muis. Hij heeft het middelste blokje kaas al opgegeten. De muis wil zich een weg eten door de kubus van kaas door steeds naar aangrenzende blokjes kaas te gaan en deze op te eten. Hij mag dus niet langs een blokje dat hij al eerder opgegeten heeft en hij mag niet buiten de kubus komen. Kan hij alle blokjes kaas opeten?*

Uitwerking Kleur de blokjes om en om zwart en wit, zodat het middelste blokje, waar de muis zit, wit is. Dan zijn er totaal 13 witte blokjes en 14 zwarte. De muis kan van zwart alleen naar wit en van wit alleen naar zwart. Hij begint met wit, dus na alle 13 witte blokjes opgegeten te hebben, zijn er nog twee zwarte blokjes over. Hij kan er daar slechts één van opeten, omdat hij niet van zwart naar zwart kan. Dus de muis kan niet de hele kubus van kaas opeten. □

Opgave 10 *Is het mogelijk een rechthoek van 16×9 vakjes te onderverdelen in 24 stenen van 1×6? (uit* Mijn Mooiste Mathe *van Leon van den Broek)*

Uitwerking Om dit probleem op te lossen, kleuren we het 16×9-bord als volgt met zes kleuren:

a	b	c	d	e	f	a	b	c
b	c	d	e	f	a	b	c	d
c	d	e	f	a	b	c	d	e
d	e	f	a	b	c	d	e	f
e	f	a	b	c	d	e	f	a
f	a	b	c	d	e	f	a	b
a	b	c	d	e	f	a	b	c
b	c	d	e	f	a	b	c	d
c	d	e	f	a	b	c	d	e
d	e	f	a	b	c	d	e	f
e	f	a	b	c	d	e	f	a
f	a	b	c	d	e	f	a	b
a	b	c	d	e	f	**a**	**b**	**c**
b	c	d	e	f	a	**b**	**c**	**d**
c	d	e	f	a	b	**c**	**d**	**e**
d	e	f	a	b	c	**d**	**e**	**f**

Aangezien elke 1×6-steen, hoe je hem ook neerlegt, alle 6 de kleuren bedekt, zouden die kleuren hier in evenwicht moeten zijn: 24 vakjes van elke kleur. Nu kunnen we gewoon kleuren gaan tellen en zien dat het niet klopt. Een snelle manier van kleuren tellen is de linker 16×6 opvullen met 1×6-stenen. Hetzelfde kunnen we doen met het rechter 12×3-gedeelte (stenen liggen over dwars nu). In het niet vet gedrukte gedeelte komt elke kleur dus 22 keer voor. In het wel vet gedrukte gedeelte komen kleur **a** en **f** te weinig voor en kleur **c** en **d** juist teveel. Dus komen niet alle kleuren evenveel voor en daarom is het onmogelijk het bord te bedekken met 1×6-stenen.
Generalisatie: met $1 \times n$-stenen kun je alleen maar flauwe rechthoeken leggen: de lengte of breedte van die rechthoek moet een n-voud zijn. □

Opgave 11 *Laat zien dat je een* 10×10*-bord niet kunt bedekken met* 1×4*-stenen.*

Uitwerking Je hebt 25 van deze stenen nodig om het bord te bedekken. Deel het bord in in 2×2-vierkantjes en kleur deze om en om zwart en wit. Elke 1×4-steen bedekt dan precies twee zwarte vakjes. Totaal bedekken 25 van deze stenen dus 50 zwarte vakjes. Echter, er zijn 52 zwarte en 48 witte vakjes (of andersom). Dus we kunnen het bord niet bedekken met deze stenen. (Er zijn allerlei andere kleuringen die ook werken.) □

Opgave 12 *Hoeveel bakstenen van 1 bij 1 bij 4 passen in een kubusvormige doos met zijde 6?*

Uitwerking Deel de doos op in $2 \times 2 \times 2$-kubusjes en kleur deze om en om zwart en wit. Totaal hebben we dan $8 \cdot 14 = 112$ zwarte blokjes en $8 \cdot 13 = 104$

witte blokjes (of andersom). Elke baksteen neemt twee witte en twee zwarte blokjes in beslag. Er kunnen dus maximaal 52 bakstenen in de doos. Het is makkelijk in te zien dat er ook 52 in passen. □

Opgave 13 *Een rechthoekige vloer is bedekt met een combinatie van* 1×4*- en* 2×2*-tegels. Als we één tegel vervangen door een tegel van de andere soort, kunnen we dan nog steeds de vloer bedekken?*

Uitwerking Nummer de rijen en kolommen en kleur een vakje zwart als het rijnummer en het kolomnummer allebei even zijn. Elke 2×2-tegel bedekt dan precies één zwart vakje. Elke 1×4-tegel bedekt ofwel geen zwarte vakjes ofwel precies twee zwarte vakjes. Als we dus een tegel vervangen door een tegel van de andere soort, dan kunnen we een zwart vakje meer of een zwart vakje minder bedekken, maar niet precies evenveel zwarte vakjes. Dus we kunnen de vloer niet meer bedekken. □

Opgave 14 *Op een* 8×8*-schaakbord zijn alle vakjes wit gekleurd op één zwart vakje na. Je mag elke rij en elke kolom herkleuren, d.w.z. elk vakje in zo'n rij of kolom wordt wit als het zwart was en zwart als het wit was. Kun je alle vakjes wit krijgen?*

Uitwerking Als in een rij of kolom eerst k vakjes zwart waren, dan zijn er na het herkleuren $8 - k$ vakjes zwart. De pariteit van het aantal zwarte vakjes verandert dus niet. Aanvankelijk is er één zwart vakje. Het is dus onmogelijk om uiteindelijk nul zwarte vakjes te krijgen. □

Opgave 15 ***(Zie inleiding, opgave 2)*** *In een rij van tien bomen zitten tien spreeuwen, in elke boom één. Op het moment dat een spreeuw een willekeurig aantal* k *bomen naar rechts vliegt, vliegt een andere spreeuw* k *bomen naar links. Kunnen alle spreeuwen uiteindelijk in één boom terecht komen?*

Uitwerking Nummer de bomen van links naar rechts met de getallen 1 t/m 10 en bekijk op elk moment de som van de boomnummers als je die optelt voor alle spreeuwen samen. (Een boomnummer kan vaker in deze som voorkomen, namelijk als er meerdere spreeuwen in die boom zitten.) Deze som is invariant onder het heen en weer vliegen, want als van de ene spreeuw het boomnummer met k toeneemt, neemt van de andere spreeuw het boomnummer juist met k af. In het begin is deze som $1+2+\cdots+10 = 55$. Als de spreeuwen uiteindelijk allemaal in boom b terecht zouden komen, zou deze waarde $b+b+\cdots+b = 10b$ zijn. Maar dan zou $10b = 55$, wat in tegenspraak is met het feit dat 55 geen 10-voud is. □

Opgave 16 *Op een eiland wonen 13 grijze, 15 bruine en 17 rode kameleons. Als twee kameleons met verschillende kleuren elkaar tegenkomen, veranderen*

ze hun kleur in de derde kleur. Kunnen op een gegeven moment alle kameleons dezelfde kleur hebben?

Uitwerking Zij G het aantal grijze en B het aantal bruine kameleons. Zij $T = G - B$ en bekijk wat er gebeurt met de waarde van T. Als een grijze en een bruine kameleon elkaar tegenkomen, dan worden G en B allebei 1 kleiner en verandert T niet. Als een grijze en een rode kameleon elkaar tegenkomen, dan wordt G precies 1 kleiner en B precies 2 groter, zodat T met 3 afneemt. Als een bruine en een rode kameleon elkaar tegenkomen, wordt G precies 2 groter en B precies 1 kleiner, zodat T juist met 3 toeneemt. Dus T is invariant modulo 3. Aanvankelijk is $T = 43 \equiv 1 \pmod 3$. Als alle kameleons dezelfde kleur hebben, dan zijn G en B beide 0 (mod 3) (namelijk gelijk aan 0 of 45), dus is $T \equiv 0 \pmod 3$. Deze situatie kan dus niet bereikt worden. □

Opgave 17 *De getallen 1, 2, ..., 20 staan op een krijtbord. We mogen twee willekeurige getallen a en b vervangen door het getal $ab + a + b$. Welk getal blijft er over nadat je dit 19 keer gedaan hebt?*

Uitwerking Definieer $P = \prod_{i=1}^{k}(a_i + 1)$, waarbij $a_1, a_2, \ldots, a_k$ de getallen op het bord zijn. Als we getallen a en b vervangen door $ab+a+b$, dan verdwijnen uit P de factoren $a + 1$ en $b + 1$, terwijl de factor $ab + a + b + 1$ toegevoegd wordt. Aangezien $(a + 1)(b + 1) = ab + a + b + 1$, verandert P niet. Dus het getal dat overblijft is gelijk aan $21! - 1$. □

Opgave 18 *Van een $n \times n$-bord is een aantal vakjes ziek. Deze ziekte is erg besmettelijk. Als een vakje minstens twee zijden gemeen heeft met zieke vakjes, dan wordt dat vakje zelf ook ziek. Aan het eind van de epidemie blijkt elk vakje van het bord ziek te zijn. Hoeveel vakjes waren er aan het begin minstens ziek?*

Uitwerking Tel van elk ziek vakje het aantal gezonde buren plus het aantal zijden dat dit vakje aan de rand van het bord heeft. De som hiervan over alle zieke vakjes noemen we S. Als een gezond vakje ziek wordt, dan grensde hij eerst aan minstens twee zieke vakjes. Nadat hij ziek geworden is, grenst hij dus nog aan hoogstens twee kanten aan een gezond vakje of de rand. Doordat dit vakje ziek is geworden, is S dus in elk geval niet groter geworden. Als alle vakjes ziek zijn, dan grenst geen enkel vakje meer aan een gezond vakje, dus is $S = 4n$. Dat betekent dat aan het begin van de epidemie moet gelden $S \geq 4n$. Omdat elk vakje vier zijden heeft, moet het aantal zieke vakjes in het begin minstens gelijk aan n zijn geweest. Dit aantal is ook voldoende: als alle vakjes op een diagonaal ziek zijn, dan worden uiteindelijk alle vakjes ziek. □

Opgave 19 *Elk roosterpunt $(x, y) \in \mathbb{Z}^2$ wordt gelabeld met een positief geheel getal, en wel zodanig dat voor elk punt z'n label het gemiddelde is van de labels van z'n vier buren. Bewijs dat alle labels gelijk zijn.*

Uitwerking Noem het kleinste label dat voorkomt m (principe 2), zeg in $(0,0)$. Als we met a,b,c,d de labels van de buren $(\pm 1,0)$ en $(0,\pm 1)$ aangeven, dan volgt enerzijds $a+b+c+d=4m$ en anderzijds $a,b,c,d \geq m$. Zou één van deze ongelijkheden strikt zijn, dan zou $a+b+c+d>4m$; tegenspraak. Dus $a=b=c=d=m$. Met inductie (naar de "afstand" $|x|+|y|$ tot de oorsprong) is nu in te zien dat elk label de waarde m heeft. □

Opgave 20 ***(Zie inleiding, opgave 3)*** *Gegeven zijn $2n$ punten in het vlak, geen drie hiervan op één lijn. De helft van deze punten stelt boerderijen voor, de andere helft waterputten. Bewijs dat het mogelijk is om elke boerderij door middel van een kaarsrechte weg zodanig met een unieke waterput te verbinden, dat al deze n verbindingswegen elkaar niet snijden.*

Uitwerking Voor elke mogelijke bijectie bekijken we de totale lengte van alle n wegen. Twee wegen snijden elkaar niet, of wel, en dan is het snijpunt een inwendig punt van beide wegen (anders zouden er drie punten op één lijn liggen). Bekijk nu die bijectie waarvoor deze totale lengte minimaal is (principe 1). We gaan laten zien dat deze bijectie voldoet. Zouden er immers snijdende wegen BP en $B'P'$ zijn, dan zouden we wegens de driehoeksongelijkheid een (strikt!) kortere totale lengte vinden wanneer we BP' en $B'P$ hadden gekozen. □

Opgave 21 *Gegeven is een eindige verzameling V van punten in het vlak zodanig dat elke lijn die door twee punten van V gaat, ook door een derde gaat. Bewijs dat alle punten op één lijn liggen.*
(Equivalent) Zij gegeven een eindige verzameling V van punten in het vlak zodanig dat ze niet allemaal op één lijn liggen. Bewijs dat er een lijn is die door precies twee punten van V gaat.

Uitwerking Stel dat alle punten niet op één lijn liggen. Dan is er dus een lijn door een tweetal punten en een punt dat niet op deze lijn ligt. Bekijk nu alle paren (P,ℓ) van zulke punten en lijnen. (In feite liggen er wegens het gegeven op al die lijnen zelfs drie punten.) Wegens principe 1 is er een paar met minimale afstand tussen P en ℓ. De loodlijn uit P op ℓ heeft voetpunt Q. Aangezien op ℓ minstens 3 punten uit V liggen, liggen er minstens twee aan dezelfde kant van Q, zeg B en A (in volgorde vanuit Q). Het paar (B,PA) heeft nu echter een (strikt) kleinere afstand tussen punt en lijn; tegenspraak. □

Volledige Inductie

Arnoud van Rooij (emeritus)
Radboud Universiteit Nijmegen
e-mail: W.vandeSluis@math.ru.nl

Volledige Inductie is een moeilijk begrip.

Het is mijn bedoeling, u te laten zien dat op schoolniveau het principe met vrucht duidelijk gemaakt kan worden, als je maar niet probeert het te formaliseren.

Ik stel me hierbij niet een hele cursus voor, maar iets voor één of twee uren in de klas, of extra stof voor individuele leerlingen - hoe (en zelfs "of") zoiets te realiseren valt, het zou dwaas zijn als ik u daarover ging adviseren.

Niettemin geloof ik dat het onderwerp zich leent tot verdere verdieping, binnen het bereik van de leerling. Zo maakt volledige inductie een wezenlijk deel uit van Zebra-boekje 26, "Een koele blik op de waarheid" door F. Verhulst.

1 Pierre de Fermat was, rond het jaar 1640, geïnteresseerd in de rij der priemgetallen

$$2, 3, 5, 7, 9, 11, 13, \ldots$$

Hij merkte op dat de getallen

$$\begin{aligned} 2^1 + 1 &= 3, \\ 2^2 + 1 &= 5, \\ 2^4 + 1 &= 17 \\ 2^8 + 1 &= 257, \\ 2^{16} + 1 &= 65.537, \end{aligned}$$

priemgetallen zijn, en sprak het vermoeden uit dat $2^{32}+1, 2^{64}+1, 2^{128}+1$, enz. ook wel priemgetallen zouden zijn, maar het rekenwerk was hem te machtig. (Begrijpelijk: $2^{32} + 1$ is 4.294.967.297.)

2 Een minder groot wiskunde, X, is geïnteresseerd in veelvouden van 7. Hij merkt op:

$$\begin{aligned} & 8^1 - 1 = 7 \text{ is een 7-voud,} \\ \text{en} \quad & 8^2 - 1 = 63 \text{ is een 7-voud,} \\ \text{en} \quad & 8^3 - 1 = 511 \text{ is een 7-voud,} \\ \text{en} \quad & 8^4 - 1 = 4095 \text{ is een 7-voud.} \end{aligned}$$

Verder gaat hij niet; het rekenwerk is hem te machtig. Hij spreekt echter het vermoeden uit dat $8^5 - 1, 8^6 - 1$, enz. ook wel 7-vouden zullen zijn.

3 Fermat had een *vermoeden*, geen zekerheid, en daar was hij zich terdege van bewust. En zelfs als rekenwerk hem had laten zien dat $2^{64}+1$ en $2^{128}+1$ priemgetallen waren, van het "enz." kon hij zich zo niet bevrijden.

X denkt nog eens na, en ziet dat hij zónder zwaar gereken toch verder kan. Hij weet nu dat 8^4-1 een 7-voud is. Welnu, dan

$8^5-1 = 8\cdot 8^4-1 = 8\cdot(8^4-1)+8-1 = 8\cdot(\text{7-voud})+7 = \text{7-voud},$
en dús
$8^6-1 = 8\cdot 8^5-1 = 8\cdot(8^5-1)+8-1 = 8\cdot(\text{7-voud})+7 = \text{7-voud},$
en dús
$8^7-1 = 8\cdot 8^6-1 = \ldots$

X ziet: Het gaat zo door, ook $8^{1001}-1$ en $8^{123456789}-1$ zijn 7-vouden.

4 Had Fermat ook zo'n kunstgreep kunnen toepassen? Nee, weten we inmiddels. Ongeveer honderd jaar na Fermat bewees Leonhard Euler dat $2^{32}+1$ geen priemgetal is, maar deelbaar is door 641. (De manier waarop hij dat deed, zónder noemenswaard rekenwerk, is een mirakel van vernuft.)

5 Paragraaf 2 is begrijpbaar voor ieder die weet wat "$8\cdot(8^4-1)+8-1$" betekent. Mijn these is dat Paragraaf 2 het wezen van volledige inductie toont. Ter wille van de verteerbaarheid dienen daaraan toegevoegd te worden: meer en uiteenlopende voorbeelden van hoe volledige inductie werkt, en illustraties van het nut van volledige inductie.

De voorbeelden blijven beperkt omdat we willen focussen op de volledige inductie zelf, niet afgeleid door gecompliceerd reken- en schrijfwerk.

6 Veronderstel, het is je een keer opgevallen dat

$$\begin{aligned} 1\cdot 2 = 2 &= \tfrac{1}{3}\cdot 1\cdot 2\cdot 3,\\ 1\cdot 2+2\cdot 3 = 8 &= \tfrac{1}{3}\cdot 2\cdot 3\cdot 4,\\ 1\cdot 2+2\cdot 3+3\cdot 4 = 20 &= \tfrac{1}{3}\cdot 3\cdot 4\cdot 5,\\ 1\cdot 2+2\cdot 3+3\cdot 4+4\cdot 5 = 40 &= \tfrac{1}{3}\cdot 4\cdot 5\cdot 6. \end{aligned}$$

Je vermoedt een patroon. Zet dat zich voort? Ja:

$$\begin{aligned} (1\cdot 2+\cdots+4\cdot 5)+5\cdot 6 &= \tfrac{1}{3}\cdot 4\cdot 5\cdot 6+5\cdot 6 = \tfrac{1}{3}\cdot 5\cdot 6(4+3) = \tfrac{1}{3}\cdot 5\cdot 6\cdot 7,\\ (1\cdot 2+\cdots+5\cdot 6)+6\cdot 7 &= \tfrac{1}{3}\cdot 5\cdot 6\cdot 7+6\cdot 7 = \tfrac{1}{3}\cdot 6\cdot 7(5+3) = \tfrac{1}{3}\cdot 6\cdot 7\cdot 8, \end{aligned}$$

enzovoorts.

7 Op deze manier heb je, tamelijk pijnloos, oneindig veel identiteiten bewezen. Stel nu eens, je wilt weten of

$$1\cdot 2+2\cdot 3+3\cdot 4+\cdots+99\cdot 100$$

meer is dan 10^5 (en je hebt geen rekentuig bij de hand). Je kunt daar natuurlijk achter komen door banaal rekenwerk, maar veel simpeler is de redenering van hierboven toe te passen; paradoxaal, want die levert nog een heleboel informatie op waar je niets aan gelegen is.

8 We bekijken de getallen

$$(*) \qquad \sqrt{6}, \sqrt{6+\sqrt{6}}, \sqrt{6+\sqrt{6+\sqrt{6}}}, \ldots$$

verderop worden de getallen lastig uit te schrijven, dus we korten af: Het n-de getal in regel $(*)$ noemen we x_n:

$$\begin{aligned} x_1 &= \sqrt{6}, \\ x_2 &= \sqrt{6+\sqrt{6}}, \\ x_3 &= \sqrt{6+\sqrt{6+\sqrt{6}}}, \\ &\text{enz.} \end{aligned}$$

of:

$$x_1 = \sqrt{6}, \quad x_2 = \sqrt{6+x_1}, \quad x_3 = \sqrt{6+x_2}, \ldots$$

De getallen in rij $(*)$ blijken te zijn:

$$(**) \qquad 2,499\ldots \quad 2,907\ldots \quad 2,984\ldots \quad 2,997\ldots \quad 2,999\ldots$$

9 Je ziet in $(**)$: de uitkomsten worden steeds groter. Misschien vind je het duidelijk dat het 38^e getal groter is dan het 37^e, maar zonder rekenwerk, zelfs zonder $(**)$, zie je dat aldus:

$6+\sqrt{6} > 6$, dus $\sqrt{6+\sqrt{6}} > \sqrt{6}$, m.a.w. $x_2 > x_1$;
dus $6+x_2 > 6+x_1$, dus $\sqrt{6+x_2} > \sqrt{6+x_1}$, m.a.w. $x_3 > x_2$;
dus $6+x_3 > 6+x_2$, dus $\sqrt{6+x_3} > \sqrt{6+x_2}$, m.a.w. $x_4 > x_3$;
enz.

10 $(**)$ suggereert misschien ook dat alle getallen daar kleiner dan 3 zijn; en jawel:

$6 < 9$, dus $\sqrt{6} < \sqrt{9}$, m.a.w. $x_1 < 3$;
dus $6+x_1 < 9$, dus $\sqrt{6+x_1} < \sqrt{9}$, m.a.w. $x_2 < 3$;
dus $6+x_2 < 9$, dus $\sqrt{6+x_2} < \sqrt{9}$, m.a.w. $x_3 < 3$;
enz.

11 Dikwijls is de redenering minder rechtlijnig.

$$\begin{aligned} \tfrac{1}{1\cdot 2} &= \tfrac{1}{2} \\ \tfrac{1}{1\cdot 2} + \tfrac{1}{2\cdot 3} &= \tfrac{2}{3} \\ \tfrac{1}{1\cdot 2} + \tfrac{1}{2\cdot 3} + \tfrac{1}{3\cdot 4} &= \tfrac{3}{4}. \end{aligned}$$

Om zeker te weten dat het patroon zich voortzet wil je hebben

$$(*) \qquad \frac{3}{4}+\frac{1}{4\cdot 5}\stackrel{?}{=}\frac{4}{5},\quad \frac{4}{5}+\frac{1}{5\cdot 6}\stackrel{?}{=}\frac{5}{6},\quad \frac{5}{6}+\frac{1}{6\cdot 7}\stackrel{?}{=}\frac{6}{7},\ldots$$

en dát wil je bewijzen, niet door ad hoc gereken zoals

$$\frac{3}{4}+\frac{1}{4\cdot 5}=\frac{3}{4}+\frac{1}{20}=\frac{15}{20}+\frac{1}{20}=\frac{16}{20}=\frac{4}{5},$$

maar via een algemeen schema dat verderop toepasbaar blijft en geen gebruik maakt van toevallige eigenschappen van 3, 4 of 5. Wel, de gemeenschappelijke structuur van de formules in $(*)$ is

$$(**) \qquad \frac{n-1}{n}+\frac{1}{n(n+1)}=\frac{n}{n+1}.$$

We zijn er dus als we $(**)$ kunnen bewijzen voor $n=4,5,6,\ldots$, en het is duidelijk hoe je dat doet.

12 Op een andere manier lastiger is dit. De "getallen van Fibonacci" zijn

$$1,2,3,5,8,13,21,34,\ldots$$

Op de 1 en de 2 na is in deze rij elk getal de som van zijn twee voorgangers. (Gewoonlijk wordt er nog een 1 vóór gezet: $1,1,2,3,\ldots$, maar dat komt hier slecht uit.)

- Bewering:

$$2>\sqrt{2}\cdot 1,\quad 3>\sqrt{2}\cdot 2,\quad 5>\sqrt{2}\cdot 3,\quad 8>\sqrt{2}\cdot 5\ ,\ldots$$

ofwel, als we het n-de getal van Fibonacci f_n noemen:

$$f_{n+1}>\sqrt{2}\cdot f_n \quad \text{voor } n=1,2,3,\ldots$$

U ziet het probleem. Volgens de standaard-formulering van het principe van volledige inductie zou je moeten bewijzen dat de ongelijkheid geldt voor $n=1$ - wat geen kunst is - en dat uit de juistheid voor een zekere n de juistheid voor $n+1$ geldt - en daar zit de kneep, want f_{n+1} wordt niet bepaald door f_n alleen maar door f_n en f_{n-1} samen.

Toch gaat het wel. Als je de eerste twee ongelijkheden eenmaal met bruut geweld bewezen hebt, kun je zó verder:

$$5=3+2>\sqrt{2}\cdot 2+\sqrt{2}\cdot 1=\sqrt{2}\cdot(2+1)=\sqrt{2}\cdot 3,\ \text{en dus}$$
$$8=5+3>\sqrt{2}\cdot 3+\sqrt{2}\cdot 2=\sqrt{2}\cdot(3+2)=\sqrt{2}\cdot 5,\ \text{enz.}$$

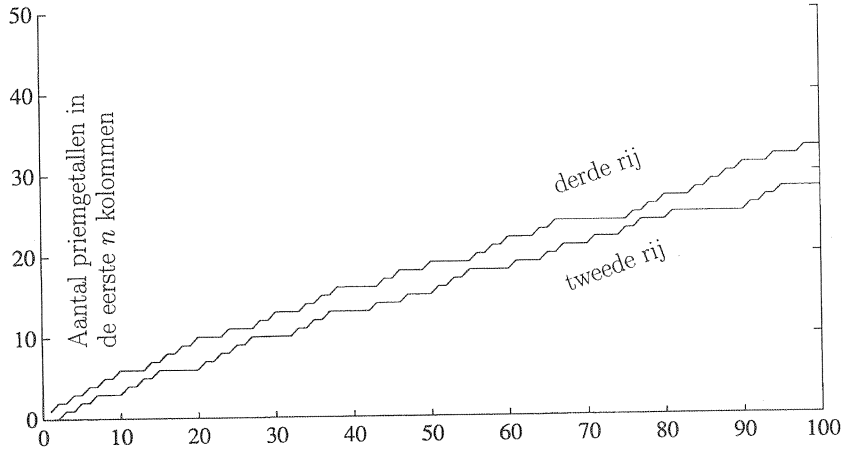
- Net zo:

$$f_{n+1}<\sqrt{3}\cdot f_n \quad \text{voor} \quad n=1,2,3,\ldots$$

13 Volledige inductie is niet de enige manier om iets over natuurlijke getallen te bewijzen. De formule

$$1+2+3+\cdots+n=\frac{1}{2}n(n+1)$$

bewijs je gemakkelijker met het plaatje op de volgende bladzijde.



14 Waar is volledige inductie goed voor? Om dat te (laten) zien moet je beschikken over een aantal voorbeelden waarin het blote idee van "zo gaat het door" naar een dwaalspoor voert. Het verhaal van Fermat is zo'n voorbeeld, maar het is niet spectaculair. Een beetje flauw is:

$$\begin{aligned} 1^0-1^1+1^2&=2^1-1,\\ 2^0-2^1+2^2&=2^2-1,\\ 3^0-3^1+3^2&=2^3-1, \end{aligned}$$

maar $4^0-4^1+4^2$ is geenszins 2^4-1.

15 Aardiger is het voorbeeld van Euler: Reken je

$$n^2-n+41$$

uit voor $n=1,2,3,4,\ldots,10$ dan vind je louter priemgetallen. Probeer je op goed geluk $n=20,30,40,50$: ja, hoor, priemgetallen.

Maar voor $n=41$?

16 Mijn favoriete voorbeeld is dit: Op (de omtrek van) een cirkel neem je n punten. Verbind elk punt met elk ander punt door een koorde. Zo verdeel je de cirkelschijf in een aantal gebieden. Hoeveel zijn dat er? (Je wordt geacht de punten op de omtrek zó gekozen te hebben dat binnen de cirkel nergens drie koorden door één punt gaan.)

Voor $n = 2, 3, 4, 5$ is het aantal $2, 4, 8, 16$ (voor $n = 0$ is het 1, als je wilt); maar voor $n = 6$ is het 31.

In het algemeen: $\binom{n}{0} + \binom{n}{2} + \binom{n}{4}$; maar dat is niet eenvoudig.

17 Een mooi voorbeeld, maar een waarvan de pointe buiten het bereik van de klas ligt:

We zetten de natuurlijke getallen in drie rijen, aldus:

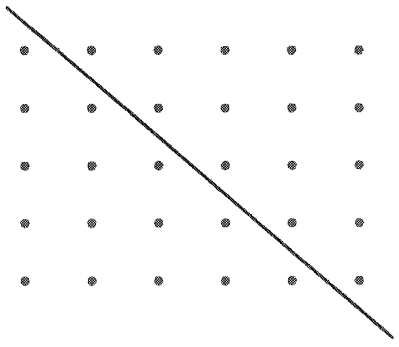
$$\begin{array}{cccc} 0 & 3 & 6 & \ldots \\ 1 & 4 & 7 & \ldots \\ 2 & 5 & 8 & \ldots \end{array}$$

en kijken in welke rijen de priemgetallen $2, 3, 5, 7, \ldots$ terechtkomen:

$$\begin{array}{cccccccccccc} 0 & \bullet & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 & 30 & 33 & \ldots \\ 1 & 4 & \bullet & 10 & \bullet & 16 & \bullet & 22 & 25 & 28 & \bullet & 34 & \ldots \\ \bullet & \bullet & 8 & \bullet & 14 & \bullet & 20 & \bullet & 26 & \bullet & 32 & 35 & \ldots \end{array}$$

In de hele eerste rij staat maar één priemgetal: 3. In de twaalf kolommen hierboven komen 4 priemgetallen voor in de tweede rij, 6 in de derde.

In een grafiekje tekenen we voor $n = 1, 2, 3, \ldots, 100$ de aantallen priemgetallen in de eerste n kolommen in de tweede en in de derde rij.



Je ziet dat de grafiek voor de derde rij overal boven die van de tweede ligt. Ga je door met grotere waarden van n, dan blijkt dit patroon zich voort

te zetten. Maar niet ten eeuwigen dage. Reken je door, dan vind je een plaats waar de grafiek van de tweede rij boven die van de derde uitkomt - voor het eerst bij $n = 202.993.937.676$, ongeveer driehonderdduizend kilometer naar rechts.

18 Een aardige is ook: Bekijk de rij $\pi, 2\pi, 3\pi, \ldots$:

$$3,1415\ldots \quad 6,2831\ldots \quad 9,4247\ldots \quad 12,5663\ldots \quad 15,7079\ldots \quad \ldots$$

Vervang wat vóór de komma staat door 0:

$$0,1415\ldots \quad 0,2831\ldots \quad 0,4247\ldots \quad 0,5663\ldots \quad 0,7079\ldots \quad \ldots$$

Je krijgt een getal tussen 0 en 1. Vermenigvuldig met 7:

$$0,9911\ldots \quad 1,9822\ldots \quad 2,9734\ldots \quad 3,9645\ldots \quad 4,9557\ldots \quad \ldots$$

Je krijgt een getal tussen 0 en 7. Neem daarvan het cijfer vóór de komma:

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad \ldots$$

Hoe gaat dit verder? Je krijgt een rij waar alleen de cijfers $0, 1, 2, 3, 4, 5, 6$, in voorkomen, dus de rij kan niet "zo doorgaan". Wat er blijkt te gebeuren is dit: Je krijgt eerst 0 t/m 6, in de gewone volgorde; dan nog eens, en nog eens ... zestien keer; dan doemt opeens een extra 6 op; dan weer zestien keer 0 t/m 6; een 6; zestien keer 0 t/m 6; en zo verder tot voorbij de duizendste term. (Het patroon moet ergens verstoord worden; dat kun je bewijzen met de irrationaliteit van π.)

19 Waarom is volledige inductie moeilijk?

De algemene formulering is als volgt. *Laat voor elk natuurlijk getal n een formule $P(n)$ gegeven zijn. Neem aan*

$$\left[\begin{array}{ll} (I) & P(0) \textit{ is juist;} \\ (II) & \textit{Als voor een natuurlijk getal } n \textit{ de formule } P(n) \textit{ juist is} \\ & \quad \textit{dan is } P(n+1) \textit{ juist.} \end{array}\right.$$

Dan is $P(n)$ juist voor elke n.

Zo gesteld is het principe van volledige inductie een ingewikkelde zin, die bovendien handelt over formules; een uitspraak over uitspraken en niet over getallen of punten of zo. We zitten hier op een hoog abstractieniveau.

Ik heb hierboven geprobeerd te laten zien hoe je dit probleem kunt ontduiken door de algemeenheid te laten schieten, en je te beperken tot demonstratie van een techniek.

20 Dan nog ligt een (heel banale) valkuil op de loer. Stel, je wilt bewijzen dat

$$2^0 + 2^1 + 2^2 + \cdots 2^n = 2^{n+1} - 1.$$

Stap I: $n = 0$: O.K.
Stap II: Neem aan: $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$; te bewijzen: $2^0 + 2^1 + \cdots + 2^{n+1} = 2^{n+1} - 1$.

"Ho!" roept een alerte leerling, "hoezo, neem aan? Dat is net wat we willen bewijzen."

Dit probleem hebben we zelf opgeroepen door nonchalant taalgebruik. Wat we willen bewijzen is niet "$2^0 + \cdots + 2^n = 2^{n+1} - 1$" maar "voor elke n geldt $2^0 + \cdots + 2^n = 2^{n+1} - 1$". Wat we onderstellen in Stap II is niet "$2^0 + \cdots + 2^n = 2^{n+1} - 1$" maar "$n$ is zó dat $2^0 + \cdots + 2^n = 2^{n+1} - 1$".

Niets aan de hand, dus, en je kunt veel verhelpen door in Stap II een andere letter dan "n" te gebruiken.

Mijn persoonlijke oplossing gaat iets verder. In Paragraaf 19 noem je een getal n "blauw" als $P(n)$ juist is; (I) en (II) worden

$$\left[\begin{array}{l} 0 \text{ is blauw;} \\ \text{elk blauw getal heeft een blauwe opvolger} \end{array}\right.$$

en het probleem is van de baan.

De uitdagende vraagstukken van bedrijven

Vivi Rottschäfer
Mathematisch Instituut
Universiteit Leiden
e-mail: vivi@math.leidenuniv.nl

1 De Studiegroep Wiskunde met de Industrie

Tijdens de jaarlijkse Studiegroep Wiskunde met de Industrie (SWI) komt een groep van ca 50 wiskundigen uit heel Nederland samen om iets anders te doen dan zij normaal doen. Gedurende een hele week werken zij samen met industriële partners aan concrete vraagstukken die vanuit de industrie ingebracht zijn. Zij bestuderen in deze week een probleem van een bedrijf en zetten de eerste stap richting een oplossing. De problemen zijn open geformuleerd, wat inhoudt dat er nog vaak een vertaalslag nodig is van het probleem naar een wiskundig model. Tijdens een SWI ligt de nadruk dan in eerste instantie vaak ook op wiskundig modelleren.

De deelnemers werken in groepen aan een probleem, waarbij er per groep specialisten uit diverse hoeken van de wiskunde samenwerken. Juist dit samenwerken blijkt een grote meerwaarde op te leveren. Het enthousiasme is daarbij zo groot dat er lang en intensief gewerkt wordt om in de korte tijd van enkele dagen tastbare resultaten te boeken. Op maandag worden de problemen aan de deelnemers gepresenteerd door de industriële partners en op vrijdag worden de resultaten en voorspellingen van de modellen gepresenteerd door de wiskundigen. Het is altijd weer verbazend hoe ver men dankzij teamwerk doorgaans komt.

De traditie van het organiseren van Studiegroepen Wiskunde met de Industrie bestaat in Nederland sinds 1998. De SWI stamt uit Engeland, waar in 1968 in Oxford de eerste Studiegroep plaats vond. Het concept werd zo'n succes, dat er tegenwoordig studiegroepen in vele landen van de wereld georganiseerd worden. In onder andere Canada, Denemarken, Australië en Engeland wordt elk jaar een SWI georganiseerd, zie ook de website http://miis.maths.ox.ac.uk. De Europese studiegroepen worden strikt doorgenummerd en de recentste SWI gehouden in 2010 op het CWI was dan ook de 72nd European Study Group with Industry.

In Nederland rouleert de SWI langs universiteiten en onderzoeksinstellingen in het land met elk jaar een andere organisatie. Deze organisatie draagt onder meer zorg voor het werven van vraagstukken bij bedrijven.

De wiskundige methodes die gebruikt worden bij het oplossen van de problemen zijn erg divers waarbij de te gebruiken aanpak vooraf vaak helemaal niet duidelijk is. Statistische methodes, optimalisatie, en het modelleren en analyseren van differentiaalvergelijkingen wordt bijvoorbeeld gebruikt. Gelukkig komen de deelnemers, van promovendus tot hoogleraar, ook uit diverse richtingen van de wiskunde.

De problemen zijn elk jaar van zeer uiteenlopende aard. De afgelopen jaren werden problemen aangedragen door onder andere de NS, KLM, Corus, ASML en diverse banken en ziekenhuizen. In alle gevallen is men tijdens en na de Studiegroep tenminste tot een gedeeltelijke oplossing gekomen, en in een aantal gevallen tot een volledige, praktisch bruikbare oplossing. Ook krijgen in sommige gevallen de projecten een vervolg in de tijd na de SWI.

2 Diverse vraagstukken

Om een indruk te geven van de diversiteit van de vraagstukken die de afgelopen jaren tijdens de SWI werden bestudeerd, zal ik eerst een korte omschrijving geven van een groot aantal problemen. Dit om een indruk te geven van de aard en de diversiteit van de problemen. Daarna zal ik iets meer in detail treden over 1 specifiek vraagstuk waaraan ik zelf heb gewerkt.

Voor de NS is er gewerkt aan rangeerproblemen met treinen. Het in de juiste volgorde combineren van treinstellen op een rangeerterrein met slechts een beperkt aantal sporen levert een ingewikkeld combinatorisch probleem op. De vraag was of we konden helpen om de tijd, de personen en de beschikbare infrastructuur zo efficiënt mogelijk te benutten.

Voor Corus werd onderzocht hoe de kwaliteit van aluminiumlegeringen verbeterd zou kunnen worden. De berekeningen die gedaan moeten worden om dat te bewerkstelligen maken gebruik van enorme hoeveelheden gegevens. Er werd een verbetering bedacht die een database van 1000 gigabytes terug wist te brengen tot 1,25 gigabytes.

Een ander probleem, waaraan ik zelf gewerkt heb, betrof een vraag van het "Waterschap Regge en Dinkel" over het analyseren van strategiëen om regenwater af te voeren. Die afvoer geschiedt via een complex netwerk van grotere rivieren en kleinere slootjes. Door analyse van afvoerpieken kon worden aangegeven waar en wanneer opslag of juist doorsluizing van water gunstig is om overstromingen te voorkomen.

KLM vroeg hoe het aantal benodigde reservedagen voor cabinepersoneel verminderd kon worden. Een zieke steward of stewardess wordt vervangen door een reserve personeelslid dat speciaal stand-by staat, maar als deze opgeroepen wordt en zijn/haar vervolgschema moet wijzigen, levert dit weer verdere verstoringen op. De vraag was of dit domino-effect verminderd kon worden.

Het Amsterdams Medisch Centrum (AMC) formuleerde een probleem wat betrekking had op de neuronen in onze hersenen. De informatie die deze neuronen versturen kan in sommige gevallen gemeten worden, maar de signalen die

daarbij gegenereerd worden zijn uitermate complex. Aan de Studiegroep de vraag of er methoden geformuleerd konden worden die de essentiële informatie uit de enorme hoeveelheid gegevens destilleren.

Om de batterijen in volgende generaties mobiele telefoons langer mee te laten gaan, worden bij NXP nieuwe transistoren onderzocht. Die zijn gebaseerd op micro-elektromechanische schakelaars die zich in meerdere niet-lineaire evenwichtstoestanden kunnen bevinden. Het berekenen van die toestanden is een lastig wiskundig probleem, dat opgelost moet worden voordat de nieuwe techniek ook daadwerkelijk toegepast kan worden.

Innogrow ontwikkelt een gesloten broeikas met ondergrondse opslag van warmte en kou. Dit bedrijf vroeg de Studiegroep te zoeken naar een methode om dit systeem te optimaliseren, door het energieverbuik te verminderen en de opbrengst te vergroten.

Het UMC in Utrecht stelde als uitdaging het optimaliseren van het electromagnetische veld in hun nieuwe MRI-scanner met een sterkte van 7 tesla, met als doel de rekentijd op een computer van vele uren naar enkele minuten terug te brengen. Dit moet het mogelijk maken het veld in redelijke tijd op de individuele patiënt af te stemmen.

De ING-bank wil, net als andere banken, de prijs van een optie snel en zorgvuldig kunnen bepalen. Dit kost veel rekentijd. Betere rekenmodellen, die zowel de rente als de beweeglijkheid van de onderliggende aandelen mee in beschouwing nemen moeten zo'n snelle prijsbepaling mogelijk maken. Aan de Studiegroep de opgave hier nieuwe richtingen in aan te geven.

3 Modelleren van een hartpomp

Tijdens de SWI van 2007 heb ik gewerkt aan een probleem geformuleerd door het Amsterdams Medisch Centrum (AMC). Samen met een groep wiskundigen en iemand van het AMC heb ik hiervoor gewerkt aan het modelleren van een hartpomp.

Bij patiënten met een acuut hartfalen, kan een klein pompje tijdelijk het pompen van het hart ondersteunen. De pomp wordt gebruikt om een deel van het bloed uit de linkerkamer de aorta in te pompen en ondersteunt zo de normale hartfunctie.

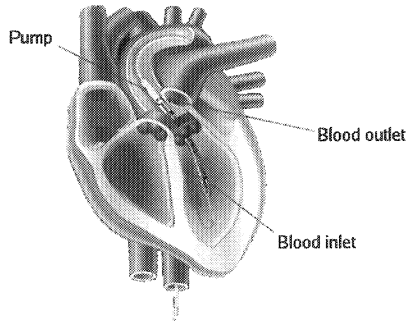
Het pompje is onder meer bedoeld voor hartpatiënten die een dotterbehandeling met een hoog risico moeten ondergaan. Tijdens het dotteren kan de pomp de bloedcirculatie dan ondersteunen. Deze patiënten lopen namelijk de kans dat ze in een cardiogene shock raken, wat gepaard gaat met een plotselinge daling van de bloeddruk, een verhoogde hartslagfrequentie, vaatvernauwing en ernstige kortademigheid.

Daarnaast wordt hetzelfde pompje ook gebruikt bij patiënten die een hartinfarct hebben gehad. Het idee is dat door de ondersteuning van het hart er minder hartspierweefsel afsterft en dat de hartfunctie beter herstelt na het infarct. In maart 2007 werden op een congres van de "American College of

Cardiology" (ACC) in New Orleans de eerste experimentele resultaten gepresenteerd.

Bij de patiënten die na het hartinfarct ondersteuning kregen van een pompje, constateerde men een belangrijke verbetering van de hartfunctie.

Er bestaan twee versies van het pompje: één die het bloed met een snelheid van 2,5 liter per minuut rondpompt, en één die een maximum haalt van 5 liter per minuut.



Figuur 1: De pomp wordt tussen de kleppen van de aorta geplaatst.

Ter vergelijking: bij een gemiddeld volwassen (gezond) persoon in rust, pompt het hart tussen 5 en 7 liter bloed per minuut rond. Het eerste pompje is vier millimeter in doorsnede en is ongeveer vijf tot zes centimeter lang. Er zit een klein motortje in, dat een soort schroef aandrijft. Het pompje wordt via de liesslagader ingebracht. Het grote voordeel van dit pompje is dat er geen ingrijpende borstkasoperatie voor nodig is om hem in het hart aan te brengen.

4 Formulering van het vraagstuk

In de periode voor de SWI kwamen resultaten en conclusies met betrekking tot de werking van het pompje alleen uit experimenten en van het plaatsen van het pompje bij patiënten. De vraag aan ons was of wij het systeem van het hart met de pomp konden modelleren aangezien er nog diverse open vragen lagen.

Bij het AMC was de afgelopen jaren bij zo'n zeventig patiënten een hartpompje ingebracht. Hoewel ze zagen dat het pompje het hart ondersteunt, wat betreft de bloedstroom en de bloeddruk, was het niet duidelijk welk deel van de bloedstroom het pompje voor zijn rekening neemt en welk deel het hart zelf verzorgt. Dat kan namelijk niet direct in de patiënt gemeten worden. Daarnaast is het onduidelijk of de huidige manier om de bloedstroom indirect te bepalen geschikt is in aanwezigheid van de hartpomp. De hartpomp verandert namelijk de bloeddoorstroming. Toch wilden ze het antwoord op deze vragen graag weten. Dan kan er namelijk bepaald worden in hoeverre een patiënt

afhankelijk is van de pomp, of de pomp harder moet werken of juist minder hard, en wanneer de ondersteuning afgebouwd kan worden, zodat het hart het bloed uiteindelijk weer helemaal op eigen kracht rondpompt.

De vraag aan de Studiegroep was dan ook of we een wiskundig model konden formuleren voor de invloed van het pompje op de cardiovasculair dynamica. De focus hierbij lag op het bepalen van de hoeveelheid bloed wat het hart zelf rondpompt, en hoeveel het pompje voor zijn rekening neemt. Aangezien dit belangrijke gegevens zijn om te kunnen bepalen in hoeverre de pomp het hart ontlast. In een experimentele omgeving, buiten het lichaam, is daar wel naar gekeken, maar eenmaal in het lichaam kan er niet exact gemeten worden wat er verandert door het aanbrengen van de pomp.

Om het model te verifiëren en om het mogelijk te maken onbekende parameters te ijken, leverde het AMC ons aan het begin van de week een exacte specificatie van de pomp, en een zogenaamde PV-loop, druk-volume kromme, van een patiënt met en een patiënt zonder pomp.

Tijdens het modelleren moesten we rekening houden met de volgende twee vereisten. Om, aan de ene kant, een realistisch model te formuleren is het belangrijk om een aantal aspecten in voldoende detail te modelleren. Dit zijn, het pompen van het hart, de dynamica van de pomp en de rest van het lichaam, met andere woorden het netwerk van aderen. Daarnaast is het belangrijk om een model te formuleren wat niet al te ingewikkeld of gedetailleerd is aangezien we een verandering van kwalitatief gedrag willen kunnen verklaren.

5 Beschrijving met elektrisch netwerk

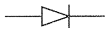
Het cardiovasculaire stelsel kan beschreven worden in termen van tamelijk complexe vloeistof dynamica. Verschillende modellen en methodes zijn hiervoor al ontwikkeld. De gebruikte numerieke technieken variëren daarbij relatief eenvoudig tot zeer geavanceerd. Helaas zijn deze niet bruikbaar omdat ze rekenintensief zijn en de flexibiliteit missen om door te rekenen wat er gebeurt als het hart van een pompje wordt voorzien.

Aangezien het blijkt dat er een grote analogie is tussen het cardiovasculaire stelsel en een elektrisch netwerk hebben wij besloten deze modelaanpak te nemen. Het is daarbij namelijk niet nodig om alle stromingsdetails van het systeem mee te nemen, die details worden in de modellering automatisch uitgemiddeld. Wel is het mogelijk om alle belangrijke componenten van het systeem mee te nemen.

Voor deze analogie representeren we het pompje als een batterij en de elasticiteit van de aderen als condensatoren. De wrijving die het bloed van de aderen voelt modelleren we als weerstanden, en de traagheid van het bloed als een spoel. Daarnaast hebben we een hartklep die dan wel open (wel stroming van het bloed), dan wel dicht (geen stroming van het bloed) is, gerepresenteerd door een diode. Zie de tabel voor de verschillende onderdelen in het hart (linker twee kolommen) en in een elektrisch circuit (rechter twee kolommen) en de

relatie ertussen.

De volgende stap was om al deze componenten goed aan elkaar te knopen zodat het elektrische netwerk inderdaad een hart met een pompje erin voorstelt. In een elektrisch netwerk worden wetten voor elektrische lading en potentiaalverschil bekeken. Voor het cardiovasculaire systeem komt de elektrische lading overeen met het bloedvolume en het potentiaalverschil is analoog aan een drukverschil. In de tabel is de gebruikte notatie in het hart als volgt:

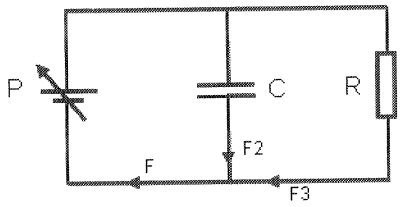
Hart			Elektrisch circuit
$P = FR_c$	vrijwing van het bloed	weerstand	$V = I R_e$
$C_c \frac{dP}{dt} = F$	elasticiteit van aderen	condensator 	$C_e \frac{dV}{dt} = I$
$L_c \frac{dF}{dt} = P$	traagheid van het bloed	magnetische spoel 	$L_e = \frac{dI}{dt} = V$
$F = \begin{cases} 0 & \text{voor } P < 0 \\ P/R_c & \text{voor } P \geq 0 \end{cases}$	hartklep	diode 	$I = \begin{cases} 0 & \text{voor } V < 0 \\ V/R_e & \text{voor } V \geq 0 \end{cases}$

P is drukverschil en F de bloedstroming. Voor een elektrisch circuit wordt de standaardnotatie gebruikt: V voor potentiaalverschil en I voor stroom. De afgeleide $\frac{d}{dt}$ geeft de verandering van de desbetreffende grootheid aan. Op een elektrisch netwerk gelden de twee wetten van Kirchhoff: behoudswetten voor lading en energie. De eerste wet van Kirchhoff stelt dat op elk punt in het netwerk de som van de in- en uitstromende ladingen gelijk aan nul is. Met andere woorden, op elk punt stroomt hetzelfde volume bloed toe als dat er weg stroomt. Volgens de tweede wet van Kirchhoff moet de som van de potentiaalverschillen in een gesloten lus gelijk aan nul zijn. Dit geeft dus aan dat de drukverschillen in het hart constant zijn.

6 Bestaande modellen

Aan de start van de Studiegroep bestonden er voor de dynamica van het hart al een aantal modellen in termen van elektrische netwerken. Modellen die wij als basis hebben genomen zijn de zogenaamde 'Windkessel' modellen.

Het eerste Windkessel model werd in 1733 geformuleerd door Stephen Hales [3]. Hij nam aan dat aderen zich gedragen zoals kamers in een ouderwetse met de hand bediende brandblusser (in het Duits *Windkessel* pomp) waarin waterpulsen omgevormd worden tot een continue straal. Door middel van bloeddruk



Figuur 2: Het 2-componenten Windkessel model.

experimenten in dieren was hij de eerste die directe metingen van bloeddruk in de aderen heeft gedaan.

De analogie van Hale tussen de waterpomp en het cardiovasculaire systeem werd later op meerdere punten uitgebreid door onder meer Otto Frank [2].

6.1 Het 2-componenten Windkessel model

Het 2-componenten Windkessel model wat Otto Frank formuleerde, is sindsdien toegepast in embryo's van kippen en ratten. Figuur 2 geeft de grafische representatie van dit model waarbij de condensator C, de elasticiteit van de aderen representeerd. Daarnaast geeft de weerstand R_p de wrijving van de bloed aan wanneer dit vanuit de aorta in nauwere vaten stroomt. De uitdrukkingen zoals geïntroduceerd in de vorige sectie leiden tot de volgende vergelijkingen

$$\begin{aligned} F &= F_2 + F_3 \\ P &= F_3 R_p \\ C\frac{dP}{dt} &= F_2 \end{aligned}$$

Eliminatie van F_2 en F_3 geeft een differentiaalvergelijking in termen van P en F

$$F = \frac{P}{R_p} + C\frac{dP}{dt}.$$

Deze vergelijking kan worden opgelost wanneer we die fase bekijken waarin de hartspieren zich ontspannen (de relaxatiefase) dan is namelijk $F = 0$. Dan vinden we

$$P = P(t_d)e^{\frac{t-t_d}{R_p C}},$$

waarbij $P(t_d)$ de bloeddruk in de aorta aan het begin van deze fase is.

6.2 Het 4-componenten Windkessel model

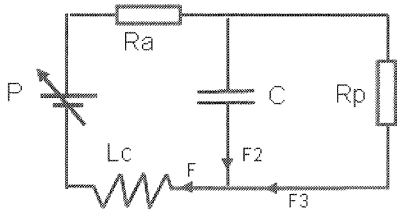
Het 2-componenten Windkessel model is in de loop der jaren uitgebreid tot een 3-componenten en uiteindelijk een 4-componenten Windkessel model. In de

jaren tachtig werd het volgende 4-componenten Windkessel model ontwikkeld voor het bestuderen van de circulatie in kippen-embryo's en voor de circulatie in de longen van katten en honden.

Voor dit model werd in het 2-componenten model een extra weerstand R_a toegevoegd die de weerstand van het bloed representeert wanneer dit de aorta-klep binnengaat. Om de traagheid van het bloed te modelleren voegen we ook een spoel toe. Deze uitbreidingen geven uiteindelijk het 4-componenten Windkessel model grafisch weergegeven door figuur 3.

De aanpak die we eerder gebruikten leidt tot de volgende vergelijking

$$(1+\frac{R_a}{R_p})F+(R_aC+\frac{L_c}{R_p})\frac{dF}{dt}+L_cC\frac{d^2F}{dt^2}=\frac{P}{R_p}+C\frac{dP}{dt}.$$



Figuur 3: Het 4-componenten Windkessel model.

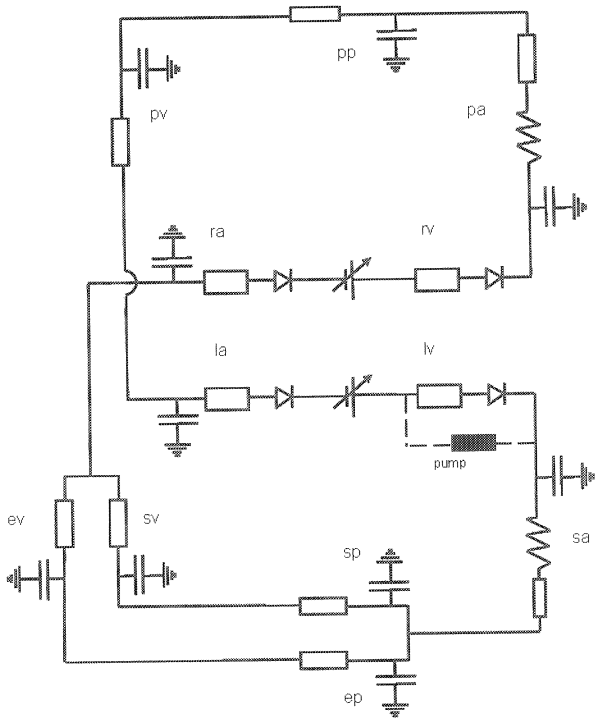
7 Uitbreiden met een pomp

Tijdens de Studiegroep hebben we de Windkessel modellen uitgebreid met de pomp. Een grafische representatie van het volledige model, wat we ontwikkeld hebben voor het hart samen met de pomp, wordt gegeven in figuur 4. Dit om een indruk te geven van de complexiteit van het model. In [1] geven we meer details van dit model en leiden we ook het bijbehorende stelsel differentiaalvergelijkingen af.

Dit stelsel van differentiaalvergelijkingen kan niet analytisch opgelost worden. De hartklep bijvoorbeeld, is een niet-lineair element, waar je analytisch niet ver mee komt. Daarom hebben we het programma Matlab gebruikt om de oplossingen numeriek te simuleren. We hebben verder aangenomen dat de pomp een constante pompsnelheid van 2,5 liter per minuut levert.

De meetgegevens die bekend zijn, zijn typisch alleen de druk en het volume van het bloed in de hartkamers. Door het modelsysteem zo te regelen dat deze meetgegevens worden gereproduceerd, dachten we de niet meetbare grootheden (hoeveel van het werk van het hart de pomp heeft overgenomen) toch op een betrouwbare manier te kunnen berekenen. Om ons model te vergelijken met uit de experimenten bekende gegevens, hebben we de druk in de linker hartkamer als functie van het volume bepaald. Dan slaagt ons model er aardig in om

de meetgegevens te reproduceren. Daarom denken we dat we de niet te meten grootheden ook aardig kunnen voorspellen. Zo hebben we de bloedstroom door de pomp als functie van de tijd berekend. Dat is waar het AMC naar zocht. Zie de proceedings voor meer details [1].



Figuur 4: Het volledige model van het hart met de pomp.

Het belangrijkste resultaat dat uit de simulaties volgt, is dat de extra weerstand die het bloed ondervindt van de pomp zelf, een belangrijke parameter in het geheel blijkt te zijn. De pomp zorgt voor een extra weerstand in de aorta. Die weerstand hangt van allerlei factoren af, en levert een niet-lineaire bijdrage. Omdat de weerstand per pomp en per patiënt kan verschillen, denken we dat er meer onderzoek nodig is om die bijdrage verder te onderzoeken.

Ook blijkt dat door de weerstand van de pomp te variëren, er een terugstroom van het bloed mogelijk is. Dan pompt de pomp te weinig bloed rond. Dit levert een sterk ongewenste situatie op, die dus voorkomen moet worden.

Verder blijkt uit de resultaten dat de pomp de bloeduitstroom van het hart onder normale omstandigheden met zeven procent vergroot: van 5,54 tot 5,95 liter per minuut. Dat is het netto resultaat van een toename van ongeveer 1,5 liter per minuut in bloeduitstroom tijdens de relaxatiefase van het hart, en een afname van ongeveer 1,1 liter per minuut in bloeduitstroom tijdens de fase waarin het hart samentrekt.

Het model kan natuurlijk nog uitgebreid worden. Aangezien het lijkt dat het huidige model de dynamica van de bloedstromen door de vaten tamelijk goed beschrijft is het daarbij niet nodig om het bloedvatenstelsel in meer detail mee te nemen. Het lijkt ons een goed idee dat verder onderzoek zich concentreert op de exacte relatie tussen de druk en de stroming door de pomp onder meer extreme omstandigheden. Het huidige model richt zich alleen op een constante pompsnelheid. Maar het model biedt ook de mogelijkheid om te onderzoeken of het variëren van de pompsnelheid misschien betere resultaten levert onder bepaalde omstandigheden.

Dank aan Vincent Creigen , Luca Ferracina, Andriy Hlod, Simon van Mourik, Michel Vellekoop en Paul Zegeling met wie ik de hele week aan dit probleem heb gewerkt. Ook dank aan Krischan Sjauw van het AMC, hij was degene die het probleem heeft voorgesteld.

Referenties

[1] Vincent Creigen, Luca Ferracina, Andriy Hlod, Simon van Mourik, Krischan Sjauw, Vivi Rottschäfer, Michel Vellekoop, Paul Zegeling (2007) Modeling a Heart Pump, *Proceedings of the fifty-eighth European Study Group with Industry*, 7 – 25.

[2] Otto Frank (1899) Die grundform des arteriellen pulses. *Zeitung fur Biologie* **37**, 483 – 586.

[3] Stephen Hales (1733) Statistical Essays II Haemostatics. Innays and Manby, London, U.K.

Boeven vangen met een Bayes net

Marjan Sjerps
Nederlands Forensisch Instituut (NFI),
Korteweg-de Vries Instituut voor Wiskunde (UvA)
e-mail: m.sjerps@nfi.minjus.nl

1 Forensische statistiek

Forensische statistiek (Forensic statistics) is een nieuwe en sterk groeiende tak van toegepaste statistiek en kansrekening, die zich concentreert op de interpretatie van (forensisch) bewijs in het strafrecht (Robertson & Vignaux 1995, Aitken & Taroni 2004, Dawid 2005, Sjerps en Coster van Voorhout 2005, Sjerps 2004, 2008, Curran 2009). Kernvragen in dit gebied zijn: Hoe groot is de bewijskracht van dit bewijsmateriaal? Wat is de bewijskracht van een combinatie van meerdere stukken bewijsmateriaal? Welke vragen kan de deskundige beantwoorden en hoe kan de jurist dit antwoord gebruiken?, Welke denkfouten worden er vaak gemaakt? De antwoorden dragen bij aan de overtuiging van de strafrechtjurist en de motivering van uitspraken.
De forensische statistiek maakt gebruik van een kansmodel om deze vragen in concrete strafzaken te beantwoorden. De ingrediënten van dit model zijn hypothesen, bewijsmateriaal, de context van de zaak, en achtergrondinformatie (NFI 2008, Berger 2010). Met het model kan de deskundige berekenen hoe de waarschijnlijkheid van de hypothesen verandert door het bewijsmateriaal.
Dit kansmodel laat zich het beste uitleggen aan de hand van een voorbeeld. Stel, bij een overval laat de dader op de plaats van het delict een bivakmuts achter. In het laboratorium wordt speeksel aangetroffen rond de mondopening van deze muts. De verdachte, Jan J., blijkt hetzelfde DNA-profiel te hebben als het speeksel. In deze zaak zullen de ingrediënten van het model als volgt worden gedefinieerd. De *context* van de zaak is hiervoor beschreven: een overval waarbij de dader een bivakmuts achterlaat, en waarbij een verdachte in beeld is. Deze context wordt gebruikt om te bepalen dat het in deze zaak zinvol is om te zoeken naar speeksel rond de mondopening, en om het DNA-profiel van het speekselspoor te vergelijken met dat van de verdachte. De *hypothesen* die de deskundige zal beschouwen zijn:

> Hypothese 1: Jan J. is de donor van het speeksel.
>
> Hypothese 2: een onbekende (niet-verwante) persoon is de donor van het speeksel.

Het *bewijsmateriaal* is de DNA-match. De *achtergrondinformatie* die in deze zaak gebruikt zal worden zijn gegevensbestanden van DNA-profielen waaruit de zeldzaamheid van het DNA-profiel van het speekselspoor kan worden bepaald. Die is bijvoorbeeld 1 op 1 miljard, d.w.z., de kans dat een willekeurig gekozen persoon dit DNA-profiel heeft is 1 op 1 miljard.
Voordat we de DNA-match in beschouwing nemen hebben de hypothesen 1 en 2 een bepaalde waarschijnlijkheid, op grond van de overige informatie in de zaak. Deze waarschijnlijkheden worden a priori kansen genoemd, om aan te geven dat het gaat om kansen vóórdat we het bewijsmateriaal beschouwen. Ze worden genoteerd als $P[H_1]$ en $P[H_2]$. De deskundige weet deze kansen niet, maar kan wel aangeven hoe zij veranderen door de DNA-match. Immers, als we de DNA-match noteren als E (van evidence), dan volgt eenvoudig uit de regel van Bayes dat

$$\frac{P[H_1]}{P[H_2]} \cdot \frac{P[E \mid H_1]}{P[E \mid H_2]} = \frac{P[H_1 \mid E]}{P[H_2 \mid E]}$$

De achtergrondinformatie wordt hierbij in alle kansen bekend verondersteld. De middelste term is bekend als het aannemelijkheidsquotiënt, 'diagnostische waarde' (Crombag et al. 1992), of Likelihood Ratio (LR).

$$LR = \frac{P[E \mid H_1]}{P[E \mid H_2]}$$

De kansen op de hypothesen nádat we het bewijsmateriaal beschouwen, de a posteriori kansen, volgen dus uit de a priori kansen door vermenigvuldiging met de LR. In de Engelstalige literatuur zie je de formule vaak terug in woorden:

prior odds x LR = posterior odds

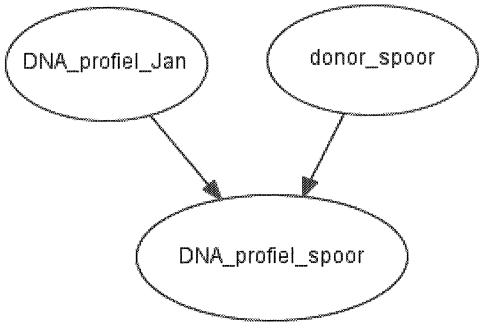
In het voorbeeld kan de deskundige berekenen dat de kansverhouding van de twee hypothesen een miljard keer groter wordt door de DNA-match. Hij kan namelijk de LR bepalen door de kans te berekenen op het vinden van de DNA-match in geval hypothese 1 waar is, en in geval hypothese 2 waar is. In geval Jan de donor is van het speeksel, zal hij altijd een match vinden (tenzij er een fout gemaakt is, bijvoorbeeld monsters verwisseld). De kans op de match is dan dus 1. In geval een onbekende persoon de donor is, zal hij vrijwel nooit een match vinden. De kans daarop is maar 1 op 1 miljard. Het quotiënt van deze twee kansen, de LR, is 1 miljard.
De teller van de LR geeft weer hoe goed het bewijsmateriaal past bij hypothese 1, en de noemer geeft weer hoe goed het past bij hypothese 2. Naarmate het bewijs beter past bij de hypothese 1 en slechter bij hypothese 2, wordt de LR groter. Andersom wordt de LR kleiner. De LR wordt daarom gebruikt als maat voor de kracht van het bewijs in het licht van de hypothesen. Voor een DNA-match tussen een spoor en de verdachte, is de LR dus een betrekkelijk eenvoudige formule. In dit geval geldt namelijk LR=1/p, waarbij p de berekende frequentie van het DNA-profiel in de

bevolking is (aannemende dat er geen fouten worden gemaakt). Deze formule is intuïtief te rechtvaardigen: we zien dat hoe zeldzamer het profiel, hoe groter de bewijskracht van de match is (ofwel hoe kleiner p, hoe groter de LR).
Bijvoorbeeld: is p gelijk aan 1 op 10, dan is de LR gelijk aan 10; is p gelijk aan 1 op 1 miljard, dan is de LR gelijk aan 1 miljard.
Net zoals er dus een maat is voor hoe hard de wind waait, (bijvoorbeeld windkracht 8 op de schaal van Beaufort), is er ook een schaal voor hoe sterk het bewijsmateriaal is (bijvoorbeeld een LR van duizend). De forensische statistiek definieert de taak van de deskundige als het rapporteren van deze LR. Veel modern forensisch onderzoek richt zich daarom op het bepalen van formules voor de LR en het vergaren van gegevens om de LR te berekenen.
Met de opkomst van het forensisch DNA onderzoek en de voortschrijdende mogelijkheden van deze techniek kwamen steeds meer moeilijke vragen op over de bewijskracht van de gevonden DNA-profielen (Meulenbroek 2009). Het aardige van bovenstaand kansmodel is dat het ook in deze meer ingewikkelde situaties goed bleek te werken. Zo is het model uitgebreid voor DNA-mengsels, verwantschaps-analyses, sporen van mindere kwaliteit waarbij er DNA-kenmerken kunnen weg-vallen, meerdere DNA-sporen, en voor de mogelijkheid van fouten (o.a. Buckleton et al. 2005). Bovendien is het model breed toepasbaar gebleken, niet alleen voor DNA maar ook voor de meeste andere forensische onderzoeksgebieden, uiteen-lopend van chemische analyses voor bijvoorbeeld de analyse van glas (Curran et al. 2002), tot de analyse van vingerafdrukken, en andere soorten van bewijs (Aitken & Taroni 2004, Sjerps en Coster van Voorhout 2005).
De forensisch statisticus richt zich dus op het afleiden van formules om de bewijskracht van forensisch bewijsmateriaal te bepalen in het licht van de relevante hypothesen. Wanneer de formules zijn afgeleid kijkt hij of er voldoende achter-grondinformatie beschikbaar is om getallen in te kunnen vullen in de formules en zodoende de bewijskracht in een getal weer te geven. In bovenstaand DNA-voorbeeld lukte dat door aan te nemen dat er geen fouten worden gemaakt in de onderzoeksketen. Verder was er een DNA-databestand aanwezig om de zeld-zaamheid van het profiel nauwkeurig genoeg te kunnen schatten. In veel gevallen is de benodigde informatie echter niet aanwezig in de vorm van nette databestanden, maar in de vorm van kennis in het hoofd van een deskundige. Deze kennis heeft de deskundige vergaard door zijn opleiding, ervaring in de zakenstroom, het doen van onderzoek en het bijhouden van nieuwe ontwikkelingen in het vakgebied. Het 'trekken' van de benodigde informatie uit het hoofd van de deskundige noemt men kenniselicitatie en is een wetenschap op zich (O'Hagan et al. 2006). Ook deze informatie kan gebruikt worden om de bewijskracht af te leiden, maar omdat kennis persoonlijk is zal de op deze wijze bepaalde bewijskracht enigszins variëren tussen deskundigen.
Behalve het ontbreken van databestanden is een andere moeilijkheid dat de uitbreiding naar meer ingewikkelder situaties leidt tot ingewikkelde formules voor de LR. De vele onzekerheden die in een echte zaak een rol spelen maken het afleiden van exacte formules vaak tot een monnikenwerk waar zelfs de doorgewinterde wiskundige geen been meer in ziet. Bovendien leiden ingewikkelde formules meestal niet tot een verhoogd inzicht. Deskundigen doen in dit soort situaties vaak een verbale uitspraak over de bewijskracht, bijvoorbeeld 'de

bevindingen van het DNA-onderzoek zijn veel waarschijnlijker wanneer er directe overdracht van DNA is dan wanneer er indirecte overdracht van DNA was' (NFI 2008). Deze uitspraak motiveren zij met een aantal argumenten, bijvoorbeeld dat er relatief veel DNA is aangetroffen, en dat je dat wel verwacht bij directe overdracht, maar niet bij indirecte overdracht. Het blijft hierbij echter vaak onduidelijk hoe de deskundige tot de kwalificatie 'veel waarschijnlijker' is gekomen en hoe de verschillende argumenten een rol spelen om te komen tot die kwalificatie.

2 Bayesiaanse netwerken

Een nieuw type modellen in de kansrekening, grafische modellen of Bayesiaanse netwerken genoemd,[1] lijkt een oplossing te kunnen bieden in een aantal van dit soort situaties (Huygen 2004, Taroni et al. 2006). De modellen zijn figuren (vandaar de naam grafische modellen) van bolletjes ('knopen') met pijlen daartussen.
Een voorbeeld van een model voor de eenvoudige DNA-match met de verdachte genaamd Jan (zie bovenstaande tekst) staat in Figuur 1.



Figuur 1: Structuur van een eenvoudig Bayesiaans netwerk voor een DNA-match tussen een spoor en de verdachte (Jan).

De 'knopen' zijn variabelen in het model, dat wil zeggen, factoren die verschillende waarden kunnen aannemen. De pijlen geven weer dat de factoren statistisch afhankelijk van elkaar zijn: als er een pijl loopt van A naar B, dan heeft informatie over A effect op de waarschijnlijkheid van B. In het voorbeeld van Figuur 1 zien we dus dat het DNA profiel van het spoor afhangt van het DNA-profiel van de verdachte Jan en van de vraag of Jan de donor is van het spoor. Als Jan namelijk de donor is, dan heeft het spoor met kans 1 hetzelfde DNA-profiel als Jan,[2] terwijl als een onbekende persoon de donor is, het spoor met kans p hetzelfde DNA-profiel heeft (bij een 'standaard' DNA-profiel is p kleiner dan 1 op 1 miljard).
Achter elke pijl van A naar B schuilt een tabel die weergeeft wat de voorwaardelijke kans is dat B een bepaalde waarde aanneemt, voor elke waarde die A kan aannemen. De kansen die men in deze tabel invult zijn natuurlijk bij voorkeur gebaseerd op

[1] Engels: graphical models, Probabilistic Expert Systems (PES), Bayesian (Belief) Networks (BBN of BN), directed acyclic graphs (DAG).
[2] Zie voetnoot 1.

'harde' data uit databases, of wetenschappelijke experimenten. Voorbeelden hiervan voor het forensisch DNA-onderzoek zijn te vinden in Bruijning-van Dongen et al. (2009) en Cowell et al. (2010). Men kan in het netwerk echter ook 'zachte' data invullen, die verkregen is via kenniselicitatie van een aantal experts. De onzekerheid van de experts over de schatting van een bepaalde kans kan daarbij ook worden verwerkt.
Met de software die voor deze modellen ontwikkeld is kan vervolgens op basis van de kanstabellen de LR eenvoudig berekend worden.[3] Ook als het model erg ingewikkeld is kan deze software de kansen doorrekenen. Zo kan een knoop A afhangen van meerdere factoren, hetgeen in het model weerspiegeld wordt door meerdere pijlen die naar knoop A lopen. De achterliggende kanstabel wordt hierdoor ook ingewikkelder, omdat nu voor elke mogelijke combinatie van de factoren de kans op A moet worden bepaald. Ik zal nu aan de hand van een denkbeeldig voorbeeld uitleggen hoe men hier in de praktijk mee om kan gaan en wat dit dan oplevert.

3 Een denkbeeldige zaak

Meneer Jansen heeft een juwelierszaak en wordt op een ochtend overvallen door een gemaskerde man die geen handschoenen draagt. Er ontstaat een worsteling tussen Jansen en de overvaller, waarbij de overvaller stevig trekt aan het colbertjasje van Jansen. Als winkelbediende Dirksen binnenkomt en de overvaller van het slachtoffer probeert los te trekken slaat de overvaller op de vlucht. Het colbertjasje van Jansen en de handen van Dirksen worden vervolgens onderzocht op DNA-sporen. De politie ontvangt een anonieme tip dat Pietersen de dader is. Op het colbertjasje van Jansen worden DNA-sporen gevonden waarvan het profiel matcht met het profiel van Pietersen. De monsters van de handen van Dirksen resulteren alleen in DNA-profielen die met Dirksen zelf matchen. De officier van justitie denkt een sterke zaak te hebben tegen Pietersen, maar die verklaart als volgt: het DNA op het jasje van Jansen kan inderdaad van hem zijn. Dat is er echter niet op gekomen tijdens de worsteling met de overvaller, maar pas daarna, en wel via de handen van winkelbediende Dirksen, die Jansen heeft helpen opstaan na de overval. Dirksen heeft namelijk die ochtend in dezelfde bus gezeten als de verdachte Pietersen, hetgeen inderdaad blijkt uit camerabeelden uit de bus. Pietersen was bovendien erg verkouden en had daardoor wellicht snot op zijn handen, dat vervolgens bij het uitstappen op een stang in de bus terecht is gekomen. Omdat Dirksen vlak daarna is uitgestapt en wellicht diezelfde stang heeft vastgepakt kan hij dus DNA van Pietersen op zijn handen hebben gekregen en dat vervolgens op het colbertjasje van Jansen gesmeerd.
Aan de DNA-deskundige wordt gevraagd of hij iets kan zeggen over de vraag hoe het DNA van Pietersen op het jasje van Jansen is gekomen: door directe overdracht tijdens de worsteling of door indirecte overdracht via de stang in de bus en de handen van Dirksen. Dat kan de deskundige inderdaad, en overweegt daarbij het

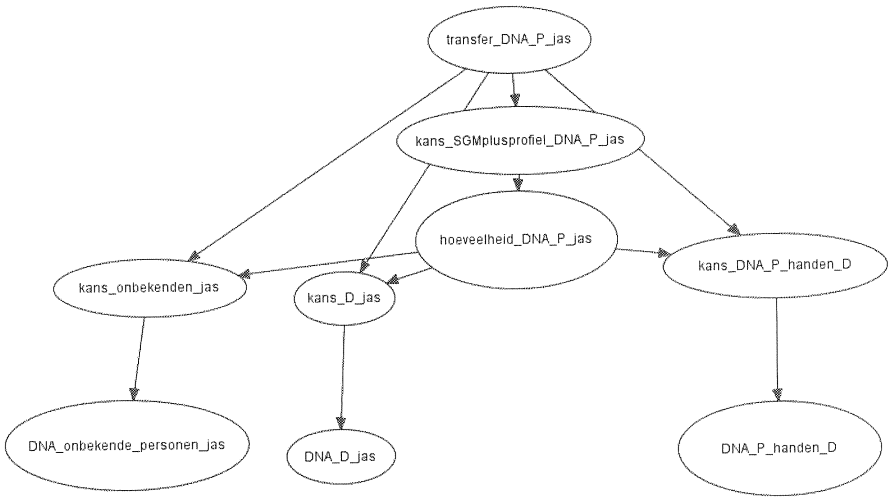
[3] Er zijn veel van dit soort programma's verkrijgbaar waarvan er een aantal, zoals GeNIe, vrij verkrijgbaar zijn via internet.

volgende. Ten eerste is er zo veel DNA van Pietersen op het jasje gevonden dat daarvan met standaardmethoden een goed profiel kon worden gemaakt. De kans dat dit lukt is relatief groot in het scenario van directe overdracht, maar is klein in het scenario van indirecte overdracht. Bovendien zat op de stang vermoedelijk DNA van andere (onbekende) personen. Het is dan, in het scenario van indirecte overdracht, opmerkelijk dat alleen het DNA van Pietersen is gevonden op het jasje van Jansen. Men zou in dit scenario ook verwachten om naast de DNA-kenmerken die matchen met de verdachte Pietersen ook DNA-kenmerken van Dirksen en DNA-kenmerken van andere personen in het DNA-profiel aan te treffen. In het scenario van directe overdracht zou men in het DNA-profiel alleen DNA-kenmerken verwachten die matchen met de verdachte. Ook het feit dat op de handen van Dirksen geen DNA wordt gevonden van Pietersen of van onbekende personen is minder goed te verklaren in het scenario van indirecte overdracht. In dat scenario, waarbij Dirksen een relatief grote hoeveelheid DNA van Pietersen op het jasje smeert, is de verwachting dat dan naderhand nog steeds DNA-kenmerken van Pietersen worden gevonden op de handen van Dirksen, waarvan bekend is dat die zijn handen niet heeft gewassen in de tijd tussen overval en bemonstering.

De deskundige neemt dus in zijn overwegingen een aantal factoren mee, en bepaalt daarbij telkens hoe groot de kans is om een bepaald DNA-profiel al dan niet waar te nemen in de verschillende scenario's. De match met het DNA-profiel van Pietersen en de hoeveelheid DNA van Pietersen, die is aangetroffen op het jasje van Jansen, zijn daarbij de meest belangrijke factoren. De hoeveelheid DNA in de bemonstering moet worden beschouwd in samenhang met de andere bevindingen van het onderzoek. Bijvoorbeeld, de kans om DNA van Pietersen aan te treffen op de handen van Dirksen in het scenario van indirecte overdracht wordt groter, naarmate er meer DNA van Pietersen op het jasje van Jansen wordt aangetroffen.

De overwegingen van de deskundige vormen hier een complex geheel. Er moeten een aantal kansen worden ingeschat en gecombineerd, die onderling samenhangen en een bepaalde mate van onzekerheid hebben. Een Bayesiaans netwerk kan in dit geval gebruikt worden om de argumenten van de deskundige te structureren en de samenhang inzichtelijk te maken.

Figuur 2 toont een dergelijk netwerk. Het probleem wordt hierbij als het ware opgeknipt in kleine stukjes, waarbij de deskundige elk stukje apart kan beschouwen.



Figuur 2: Structuur van een Bayesiaans netwerk dat de overwegingen weergeeft van de DNA-deskundige in de denkbeeldige zaak van sectie 3.

Als de deskundige alle achterliggende kanstabellen van het netwerk heeft ingevuld, kan het netwerk vervolgens de LR berekenen van het geheel aan bevindingen. De deskundige kan hiermee zijn conclusie, dat de bevindingen bijvoorbeeld 'veel waarschijnlijker' zijn in het scenario van directe overdracht, dan in het scenario van indirecte overdracht numeriek onderbouwen. Hij kan met het netwerk precies laten zien hoe hij tot zijn conclusie komt: welke aannamen maakt hij, welke factoren beschouwt hij, hoe zwaar weegt hij elke factor, en hoe beïnvloeden zij elkaar.

De deskundige kan dit model ook gebruiken om het effect van onzekerheid van zijn kansinschattingen te bepalen. Deze onzekerheid kan sterk variëren omdat bijvoorbeeld sommige overdrachtskansen goed bekend zijn uit de literatuur, terwijl over andere kansen niet veel bekend is. Ook kan de deskundige een gevoeligheidsanalyse doen om te laten zien wat het effect is van bepaalde aannamen, en wat de meest cruciale factoren bij het vaststellen van de bewijskracht zijn.

De eindconclusie van verschillende deskundigen kan in dit soort situaties van elkaar verschillen. Een Bayesiaans netwerkmodel dat door verschillende deskundigen is ingevuld kan duidelijk maken hoe groot de verschillen zijn tussen de deskundigen. Ook wordt duidelijk waaróm de deskundigen van mening verschillen: welke kansen en onzekerheden worden anders ingeschat? Het voordeel voor de rechtspraak is dat de discussie zich snel kan toespitsen op de wezenlijke punten van discussie. De jurist kan zich dan richten op de vraag welke deskundige de beste onderbouwing heeft voor de kansen die hij heeft ingevuld in het model. Een andere mogelijkheid is

om de mening van beide deskundigen in het model te verwerken en tot een soort gewogen gemiddelde te komen. Natuurlijk zijn er ook een aantal haken en ogen aan het gebruik van Bayesiaanse netwerken in het strafrecht (Sjerps & Kloosterman 2010).

4 Bayesiaanse netwerken voor de middelbare scholier

Hoewel de forensische statistiek zich concentreert op de interpretatie van forensisch bewijs zijn Bayesiaanse netwerken ook in veel bredere zin interessant voor beslisprocessen onder onzekerheid. Je kunt er bijvoorbeeld eenvoudig het beruchte drie-deuren probleem mee oplossen. In dit probleem mag de finalist van een quiz kiezen uit drie deuren, waarbij achter één deur een prijs staat en achter de twee andere deuren helemaal niets. De kandidaat zegt tegen de quiz-master dat hij deur 1 gaat openen. De quiz-master, die weet achter welke deur de prijs staat, houdt hem echter tegen en opent deur 2, waarachter geen prijs staat. Moet de finalist nu deur 1 of 3 openen, of maakt het niets uit? Op de website van Hugin (www.hugin.com) is een gratis demo-versie van het programma te downloaden. In de help-functie staat onder help-topics/examples/hugin-examples beschreven hoe je dit probleem (dat in het Engels bekend staat als 'Monty Hall') kunt oplossen met een Bayesiaans netwerk. In deze help-functie zijn nog een aantal leuke en simpele voorbeelden te vinden. Een ander populair en gratis te downloaden programma is GeNIe (via http://genie.sis.pitt.edu/networks.html). Voor wiskunde docenten zijn forensische statistiek en Bayesiaanse netten wellicht interessant om stof uit de kansrekening en statistiek op aansprekende wijze te illustreren. De slimmere scholieren zullen het zelf maken van Bayesiaanse netwerken hopelijk een leuke kluif vinden.

5 Conclusie

In de forensische statistiek bestaat een numerieke maat voor de bewijskracht van wetenschappelijke onderzoeksresultaten, de zogenaamde *Likelihood Ratio* (LR). De LR wordt in zaken waar forensisch DNA-onderzoek een rol speelt vaak daadwerkelijk uitgerekend om de wetenschappelijke bewijskracht van een DNA-match vast te kunnen stellen. Voor andere belangrijke vragen, bijvoorbeeld hoe een DNA-spoor kan zijn overgedragen worden de formules voor de berekeningen van de LR echter al snel te moeilijk. Dit geldt ook voor overdracht van andere typen forensisch bewijs of voor het bepalen van de bewijskracht van de combinatie van verschillende bewijsmiddelen. Met een nieuwe techniek uit de kansrekening, Bayesiaanse netwerken, kan de LR toch worden berekend op basis van kansinschattingen door één of meer deskundigen. Een Bayesiaans netwerk maakt hierbij bovendien de redenering inzichtelijk: welke aannamen worden gemaakt, welke factoren worden beschouwd, hoe zwaar wegen zij, hoe hangen zij samen, en op welk punt verschillen de deskundigen van mening? Voor wiskunde docenten die kansrekening moeten onderwijzen is de forensische statistiek een bron van aansprekende voorbeelden. De slimmere scholieren kunnen zelf Bayesiaanse netten maken met gratis software.

6 Referenties

[1] Aitken C.G.G. & Taroni, F. (2004). *Statistics and the evaluation of evidence for forensic scientists- 2nd* (ed). Wiley, Chichester UK.

[2] Berger, C.E.H. (2010). *Criminalistiek is terugredeneren. Logisch correct redeneren in forensische rapportages ... en in de rechtszaal.* Nederlands Juristenblad 646, pp. 784–789.

[3] Bruijning-van Dongen C.J., Slooten K., Burgers W.G., Wiegerinck W.A.J.J. (2009). *Bayesian networks for victim identification on the basis of dna profiles.* Forensic Sci. Int. Gene. Suppl., vol. Genetics Supplem, no. Series 2, pp. 466–468.

[4] Buckleton J., Triggs C.M. & Walsh S.J. (ed). (2005). *Forensic DNA evidence interpretation.* CRC Press, Boca Raton.

[5] Cowell R.G., S.L. Lauritzen & J. Mortera (2010 in press). *Probabilistic expert systems for handling artifacts in complex DNA mixtures.* Forensic Science. International: Genetics, doi:10.1016/j.fsigen.2010.03.008.

[6] Crombag H.F.M., P.J. van Koppen & W.A. Wagenaar (1992). *Dubieuze zaken: de psychologie van strafrechtelijk bewijs.* Contact, Amsterdam.

[7] Curran J.M. (2009). *Statistics in forensic science.* Wileys interdisciplinary reviews: Computational Statistics 1, pp. 141–156.

[8] Curran J.M., Hicks T.N. & Buckleton J.S. (2000). *Forensic Interpretation of Glass Evidence.* CRC Press, Boca Raton.

[9] Dawid, A.P. (2005). *Probability and proof. On-line Appendix to Analysis of Evidence (Second Edition),* by T.J. Anderson, D.A. Schum & W.L. Twining. Cambridge University Press. http://tinyurl.com/7g3bd, pp. 94.

[10] Meulenbroek A.J. (2009). *De essenties van forensisch biologisch onderzoek-Humane biologische sporen en DNA.* Uitgeverij Paris.

[11] NFI (2008). *De reeks waarschijnlijkheidstermen van het NFI en het Bayesiaanse model voor interpretatie van bewijs.* Vakbijlage, www.forensischinstiuut.nl .

[12] O' Hagan A., Buck C.E., Daneshkhah A., Eiser J.R., Garthwaite P.H., Jenkinson D.J., Oakley J.E., Rakow T. (2006). *Uncertain judgements-Eliciting expert's probabilities.* John Wiley & Sons, Chichester UK.

[13] Huygen PEM (2004). *Bayesian Belief Networks voor redeneren over juridische bewijsvoering.* In: W.H. van Boom & M.J. Borgers (red). De rekenende rechter, Boom Juridische Uitgevers, Den Haag.

[14] Robertson B. & Vignaux G.A. (1995). *Interpreting evidence-evaluating forensic science in the courtroom.* Wiley, Chichester UK.

[15] Sjerps, M. (2004). *Forensische statistiek.* Nieuw archief voor de wiskunde 5/5: pp. 106–111, zie http://www.nieuwarchief.nl/ .

[16] Sjerps, M.J. (2008). *Forensische statistiek en kansrekening: interpretatie van bewijs.* In: Forensische Expertise, A.P.A. Broeders en E.R. Muller (red.), pp. 467-496, Kluwer, Deventer.

[17] Sjerps, M.J. & J.A. Coster van Voorhout (red.) (2005). *Het onzekere bewijs. Gebruik van statistiek en kansrekening in het strafrecht.* Kluwer, Deventer.

[18] Sjerps, M.J. & Kloosterman AD (2010 in druk). *Het gebruik van Bayesiaanse netwerken in de forensische (DNA)-statistiek.* Ars Aequi.

[19] Taroni F., Aitken C., Garbolino P. & Biedermann A. (2006). *Bayesian networks and probabilistic inference in forensic science.* John Wiley & Sons, Chichester, UK.

Gênante problemen

Ionica Smeets
Liacs, Universiteit Leiden
e-mail: Ionica.Smeets@gmail.com

Gênante vragen

Mijn vriendin Cristel studeerde geschiedenis met als specialisatie achttiende-eeuwse dagboeken. Op feestjes belandt ze steevast naast iemand die werkelijk alles weet van de Peloponnesische oorlog. Als zo iemand hoort dat zij een historica is, dan verwacht hij dat ze daar uren met hem over kan praten. Cristel vindt het dan altijd een beetje gênant om toe te moeten geven dat zij helemaal niets weet van de Peloponnesische oorlog.

Als wiskundige kom je bijna nooit in zulke situaties, omdat de meeste mensen bij wiskunde niet verder komen dan de stelling van Pythagoras. Daarom was ik zo verbaasd toen iemand laatst op een borrel aan me vroeg hoe het zat met het vermoeden van Collatz.

Ik wist gelukkig wel wat het vermoeden van Collatz was. Het gaat over reeksen getallen. Je begint met een willekeurig geheel getal, groter dan nul. Als het getal even is, dan deel je het door twee. Als het getal oneven is, dan vermenigvuldig je het met drie en tel je er één bij op. Daarna herhaal je dit proces met de uitkomst, en opnieuw, en opnieuw. Bijvoorbeeld:

$$6 \to 3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$$

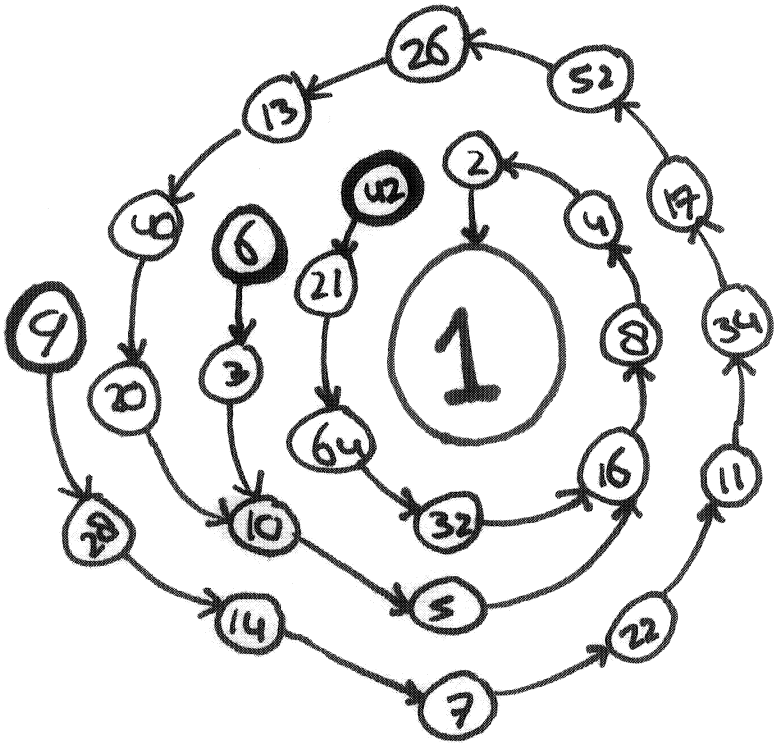
of

$$13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1.$$

Je stopt bij één, omdat je vanaf daar in een vicieuze cirkel belandt: één gaat immers naar vier en dan via twee weer terug naar één. Het vermoeden van Collatz is dat je altijd op één uitkomt, met welk getal je ook begint.

Probeer het zelf maar eens voor je lievelingsgetal. Als je getal kleiner is dan 10^18 dan kom je zeker op één uit, tot die grens is het vermoeden met de computer getest. Het aantal stappen kan behoorlijk groot worden: als je begint met een bescheiden 27 heb je bijvoorbeeld al 112 stappen nodig voor je bij 1 eindigt.

De meeste wiskundigen denken dat het vermoeden van Collatz waar is en dat je inderdaad voor elk getal bij één zult eindigen. Maar niemand heeft een bewijs. De in 1996 overleden wiskundige Paul Erdös verzuchtte volgens de overlevering



Figuur 1: De reeksen die je krijgt als je begint bij 6, 9 of 42.

dat de wiskunde nog niet klaar was voor dit soort moeilijke problemen. Voor de zekerheid loofde hij toch maar 500 dollar uit voor een oplossing. Die oplossing is er nog steeds niet.

Dit alles vertelde ik op de borrel. De getallenvoorbeelden zocht ik snel op met mijn telefoon, iets wat ik ook van harte aanraad bij lastige vragen over Peloponnesische oorlogen. De vragensteller keek me wat teleurgesteld aan. Dus dit kunnen wiskundigen niet oplossen? Wat zitten jullie dan de hele dag achter jullie bureaus te doen? En wat kunnen jullie wel?

Het is misschien gênant om een vraag te krijgen over een onderwerp waarvan je nog nooit hebt gehoord. Maar het is nog veel gênanter om toe te moeten geven dat jij en je vakgenoten een ogenschijnlijk eenvoudig probleem niet kunnen oplossen.

Gênante problemen

Het voorgaande stuk schreef ik als column voor De Volkskrant. Ik heb daarin een beetje gelogen (diverse columnisten drukten mij op het hart om vooral veelvuldig te liegen in columns). Nog nooit vroeg iemand mij op een feestje naar het vermoeden van Collatz (Cristel bestaat trouwens wel en zij krijgt echt altijd lastige vragen, zij het niet per se over Peloponnesische oorlogen). Ik was geïnteresseerd geraakt in gênante problemen door een stukje op de blog van Richard Lipton [4]. Daar beschrijft hij wiskundige problemen die zo eenvoudig klinken dat je niet kunt geloven dat ze nog steeds niet zijn opgelost. Lipton noemt zelf een aantal voorbeelden en in de reacties komen wiskundigen enthousiast met allerlei suggesties. Vlak nadat ik dat artikel las, vertelde ik op een diner over dat soort problemen aan een paar niet-wiskundige vrienden. En toen vroeg iemand echt "Dus dit kunnen wiskundigen níet oplossen? Wat zitten jullie dan de hele dag achter jullie bureaus te doen? En wat kunnen jullie wél?". Dus ik hoefde niet eens zoveel te liegen in mijn column.

Zelf vind ik het wel hoopgevend dat er nog allerlei eenvoudig klinkende, onopgeloste wiskundige problemen zijn. De Riemann-hypothese is zo moeilijk dat hij nauwelijks aan buitenstaanders is uit te leggen. Maar dit soort problemen zijn vaak zo toegankelijk dat je ze aan je moeder uit kunt leggen en daarna gelijk zin krijgt om samen op een servetje een oplossing te zoeken. Bekende voorbeelden zijn het vermoeden van Goldbach (elk even getal groter dan twee is te schrijven als de som van twee priemgetallen) en bovenstaand vermoeden van Collatz. Maar er zijn nog veel meer van dit soort problemen. Voor wie meer wil lezen over het vermoeden van Collatz, is er een prachtig overzichtsartikel van Jeff Lagarias [2]. Maar nu dus wat andere problemen.

Vragen over π

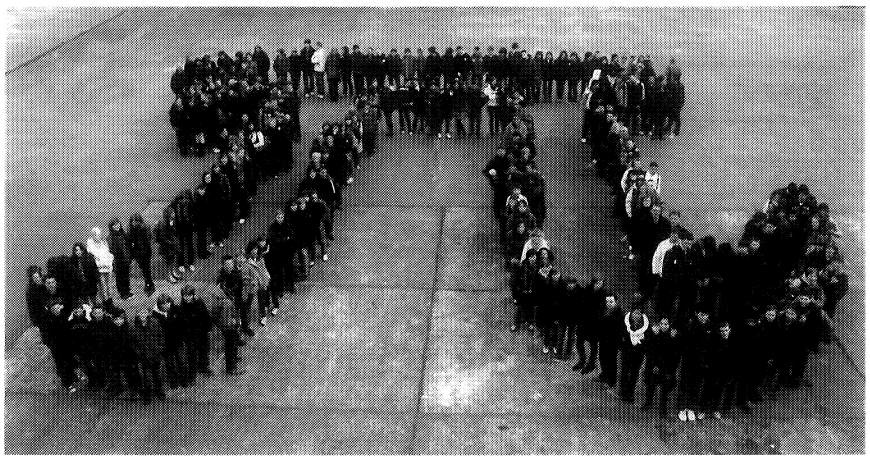
We weten een heleboel over π, de verhouding tussen de omtrek en diameter van een cirkel. We weten bijvoorbeeld dat π geen breuk is, oftewel dat π een irrationaal getal is. Van de oneindig veel decimalen van π hebben we inmiddels de eerste 2,7 biljoen cijfers uitgerekend. Maar over die decimalen weten we ook een heleboel dingen *niet*. Zitten er oneindig veel enen in de decimalen? Geen idee. Komt elk getal even vaak voor? Niemand die het zeker weet.

Algebraïsche en transcendente getallen

Een *algebraïsch getal* is te schrijven als de oplossing van een vergelijking van de vorm

$$c_n x^n + c_{n-1} x^{n-1} + \ldots + c_2 x^2 + c_1 x + c_0 = 0, \tag{1}$$

waarin alle c_i gehele getallen zijn.



Figuur 2: Met deze foto won KSO Glorieux Ronse in 2009 de pi-fotowedstrijd.

Bijvoorbeeld $\sqrt{2}$ is een algebraïsch getal, omdat het een oplossing is van

$$x^2 - 2 = 0.$$

Een getal dat niet te schrijven is als de oplossing van een vergelijking van de vorm (1), noemen we *transcendent*. Het is een stuk makkelijker om van een getal te laten zien dat het algebraïsch is (je hoeft alleen een vergelijking te geven), dan om te bewijzen dat een getal transcendent is.

Eén van de bekendste transcendente getallen is de constante van Liouville c

$$c = \sum_{j=1}^{\infty} 10^{-j!} = 0,110001000\ldots,$$

waarbij er enen staat op de plaatsen $1, 2, 6, 24, 120, 720, \ldots$, oftewel $1!, 2!, 3!, 4!, 5!, 6!, \ldots$ (waarbij $j! = j \cdot (j-1) \cdot (j-2) \cdots 3 \cdot 2 \cdot 1$).

De constante is een voorbeeld van een Liouville getal: een reëel getal x met de eigenschap dat voor elk positief getal n er gehele getallen p en $q > 1$ bestaan zo dat

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}.$$

Om te zien dat de constante van Liouville inderdaad een Liouville getal is, neem je voor een gegeven n

$$p_n = \sum_{j=1}^{n} 10^{n!-j!} \quad \text{en} \quad q_n = 10^{n!}.$$

Dan geldt

$$\left|c - \frac{p_n}{q_n}\right| = \sum_{j=n+1}^{\infty} 10^{-j!} = 10^{-(n+1)!} + 10^{-(n+2)!} + \ldots < 10 \cdot 10^{-(n+1)!} \leq (10^{-n})^n = \frac{1}{q_n^n}.$$

Het is niet zo moeilijk om te laten zien dat elk Liouville getal irrationaal is (huiswerk voor de liefhebber). In 1844 bewees Joseph Liouville bovendien dat al deze naar hem vernoemde getallen transcendent zijn, waarmee hij voor het eerst aantoonde dat er daadwerkelijke transcendente getallen bestaan.

Figuur 3: Joseph Liouville, de man die als eerste een transcendent getal kon aanwijzen.

Het bewijs dat we hier geven gebruikt het volgende lemma.

Lemma 1. *Als x een irrationaal getal is dat een nulpunt is van een polynoom met graad $n > 0$, dan bestaat er een reëel getal $A > 0$ zo dat voor alle gehele getallen $p, q > 0$ geldt*

$$\left|x - \frac{p}{q}\right| > \frac{A}{q^n}.$$

Het bewijs van dit lemma is te vinden op wikipedia [5] of in het mooie boekje [3]. De volgende stelling bewijst met hulp van dit lemma uit het ongerijmde dat alle Liouville getallen transcendent zijn.

Stelling 2. *Elk Liouville getal is transcendent.*

Bewijs. Laat x een Liouville getal zijn een neem aan dat x algebraïsch is. Dan bestaan er volgens Lemma 1 een geheel getal n en een reëel getal $A > 0$, zodat voor alle gehele getallen p en $q > 1$ geldt

$$\left|x - \frac{p}{q}\right| > \frac{A}{q^n}.$$

Kies nu een positief getal r zodat $\frac{1}{2^r} \leq A$ en zet $m = r + n$. Omdat x een Liouville getal is, bestaan er gehele getallen p en q zodat

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^m} = \frac{1}{q^{r+n}} < \frac{1}{2^r} \frac{1}{q^n} \leq \frac{A}{q^n},$$

wat een tegenspraak geeft met het lemma. Dus we concluderen dat x niet algebraïsch is en dus transcendent moet zijn. □

π en e

Het bewijs dat alle Liouville getallen transcendent zijn is al wat gedoe, bewijzen dat π transcendent is, is nog een stuk lastiger. Maar inmiddels is bewezen dat zowel π als e transcendente getallen zijn. Maar (en nu komt er weer een gênant probleem), zijn $\pi - e$ en $\pi + e$ transcendent? Wederom niemand die het weet. Wat het nog pijnlijker maakt, is dat we zeker weten dat minstens één van deze getallen transcendent is, want als ze allebei algebraïsch waren, dan zou

$$\frac{1}{2}(\pi + e + \pi - e) = \pi$$

dat ook moeten zijn.

Om een zelfde reden, weten we ook dat $\pi + e$ of πe transcendent moet zijn. Is het niet gênant dat we wel kunnen bewijzen dat π en e transcendent zijn, maar dat we met onze handen in het haar zitten bij de toch niet zo veel moeilijker lijkende getallen $\pi - e, \pi + e$ en πe?

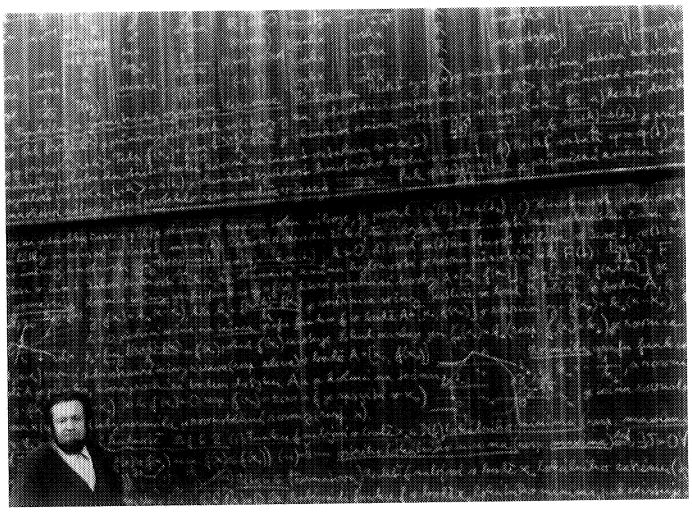
Het vermoeden van Zaremba

Mijn eigen favoriete gênante probleem is het vermoeden van Zaremba. Het werd mij verteld op een conferentiediner door de Japanse wiskundige Shigeki Akiyama. Hij zei tegen me: "Als je hier drie maanden aan werkt, dan word je een echte wiskundige."

Het vermoeden gaat over kettingbreuken. Elk reëel getal x is te schrijven in de vorm

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots}}}},$$

waarbij a_0 een geheel getal is en alle andere a_i positieve gehele getallen zijn. Als x een irrationaal getal is, dan is de kettingbreuk oneindig en uniek. De meeste resultaten over kettingbreuken zijn voor irrationale getallen. Het vermoeden van Zaremba gaat juist over gewone breuken.



Figuur 4: Voorbeeld van een echte wiskundige.

Elk rationaal getal heeft een eindige kettingbreuk. Die kun je op twee manieren eindigen, omdat voor elk geheel getal a_n geldt

$$\frac{1}{a_n} = \frac{1}{a_n - 1 + \frac{1}{1}}.$$

Hierbij moet je altijd even afspreken welke van de twee vormen je als standaard kiest.

Het vermoeden van Zaremba is dat er een constante B bestaat zodat voor elk positief getal q er een positief getal $p < q$ bestaat (waarbij p en q grootste gemene deler 1 hebben), zodat voor alle a_i in de kettingbreuk van

$$\frac{p}{q} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

geldt dat $a_i < B$.

Neem bijvoorbeeld $q = 12$ en kijk dan naar de kettingbreuken van $\frac{1}{12}, \frac{5}{12}, \frac{7}{12}$ en $\frac{11}{12}$.

$$\frac{1}{12} = \frac{1}{12}, \quad \frac{5}{12} = \frac{1}{2+\dfrac{1}{2+\dfrac{1}{2}}}, \quad \frac{7}{12} = \frac{1}{1+\dfrac{1}{1+\dfrac{1}{2+\dfrac{1}{2}}}} \quad \text{en} \quad \frac{11}{12} = \frac{1}{1+\dfrac{1}{11}}.$$

We zien hier dat $B = 3$ voldoende is omdat alle a_i in de kettingbreuk van $\frac{5}{12}$ (en ook in die van $\frac{7}{12}$) kleiner zijn dan 3. In het algemeen vermoeden we dat $B = 5$ zal werken voor alle natuurlijk getallen q, maar bewijzen zitten daar nog mijlen vandaan [1].

Helaas moest ik in de tijd dat ik het vermoeden van Zaremba hoorde mijn proefschrift afmaken en ook daarna had ik geen tijd om aan dit vermoeden te werken. Maar ooit, als ik met pensioen ga, dan maak ik drie maanden vrij voor dit vermoeden en zal ik (eindelijk) een echte wiskundige worden.

Referenties

[1] T.W. Cusick, Zaremba's conjecture and sums of the divisor function. *Mathematics of Computation*, 61:171–176, 1993.

[2] Jeff Lagarias, `http://www.cecm.sfu.ca/organics/papers/lagarias/`. Eerder verschenen in *American Mathematical Monthly* 92: 3 – 23,1985.

[3] Ivan Niven, Irrational numbers. Carus Mathematical Monographs, The Mathematical Association of America, 2005 (origineel uit 1956).

[4] R.J. Lipton, Mathematical embarrassements. `http://rjlipton.wordpress.com/2009/12/26/mathematical-embarrassments/`

[5] Liouville number. `http://en.wikipedia.org/wiki/Liouville_number`

Hoe je het cryptosysteem RSA soms kunt kraken

Benne de Weger
Technische Universiteit Eindhoven
http://www.win.tue.nl/~bdeweger/
e-mail: b.m.m.d.weger@tue.nl

1 Inleiding

1.1 RSA

RSA is een veelgebruikt cryptografisch systeem, bijvoorbeeld voor het beveiligen van internetverkeer. Het is een asymmetrisch systeem, d.w.z. versleutelen gebeurt met een publieke sleutel, ontsleutelen met de bijbehorende privé-sleutel. RSA maakt gebruik van eenvoudige getaltheorie en kan dan ook goed behandeld worden in een keuzeonderwerp Cryptografie bij Wiskunde D[1]. In de Vakantiecursus 2008 heeft Lenny Taelman [T] de basis van RSA besproken. Een recent Nederlandstalig boek dat een inleiding geeft tot de wiskunde van de asymmetrische cryptografie is [W1], zie ook [B, hst. 9], [Ke, par. 13.5].

De publieke sleutel – de naam zegt het al – mag iedereen weten. De privé-sleutel zal de eigenaar strict geheim willen houden. Zo kan iedereen iets versleutelen wat alleen de eigenaar van het sleutelpaar weer leesbaar kan maken. Omdat de publieke sleutel publiek is, maar wel samenhangt met de privé-sleutel, kun je je afvragen of de publieke sleutel niet genoeg informatie biedt om de privé-sleutel uit af te kunnen leiden. Dat zou natuurlijk niet moeten. Dat dat inderdaad praktisch onmogelijk is, is gebaseerd op het feit dat het ontbinden van grote getallen in priemfactoren een erkend (maar onbewezen) moeilijk probleem is. Verder moet de privé-sleutel op een veilige plek bewaard worden, bijvoorbeeld op smartcard, omdat goede smartcards niet zomaar uit te lezen zijn.

RSA heeft een goede reputatie als een zeer veilig systeem. Maar onder bepaalde omstandigheden is RSA wel degelijk te kraken. Gelukkig zijn deze omstandigheden makkelijk te vermijden, maar je wilt toch graag weten waar je aan toe bent. In deze cursus zullen enkele technieken om onder voorwaarden RSA te kunnen kraken geïllustreerd worden aan de hand van voorbeelden.

[1] Lesmateriaal over cryptografie voor Wiskunde D is o.m. te vinden bij het Steunpunt Wiskunde D van de TU/e, http://www.win.tue.nl/wiskunded.

1.2 Soms te kraken

Na kort RSA besproken te hebben in hoofdstuk 2, gaan we als eerste kijken naar zwakke sleutels. In Euclides van juni/juli 2009 is daar ook over geschreven [W2], en in deze cursus gaan we daar dieper op in. Met name de zogenaamde "privé-exponent" moet niet te klein gekozen worden. We laten in hoofdstuk 3 zien hoe kettingbreuken een rol spelen bij het kraken van RSA als deze privé-exponent te klein is, en in hoofdstuk 4 zien we hoe een geavanceerdere techniek daarin nog wat verder komt. Deze techniek is het zoeken van kleine nulpunten van polynomen in twee variabelen.

Vervolgens gaan we in hoofdstuk 5 uit van de omstandigheid dat een deel van de privé-sleutel gelekt is. Dat zou bijvoorbeeld kunnen door het stroomgebruik van de smartcard te meten terwijl die berekeningen doet met de privé-sleutel. Als een voldoende groot deel van de privé-sleutel (bijvoorbeeld van de privé-exponent, of van de priemfactoren van het te ontbinden getal) bekend is, kan de rest berekend worden. Ook hier gaat dat met het zoeken van kleine nulpunten van polynomen in twee variabelen.

Tenslotte kijken we in hoofdstuk 6 naar een situatie waarbij expres een foutje in de privé-sleutel geïntroduceerd wordt. Dat kan bijvoorbeeld door een smartcard even in de magnetron te leggen. We laten zien hoe de originele privé-sleutel kan lekken door de zo mishandelde smartcard een berekening te laten doen.

2 RSA

2.1 Een sleutelpaar

Een RSA-sleutelpaar wordt als volgt gemaakt.

- Maak twee willekeurige priemgetallen p en q, en bereken hun product $n = pq$. Deze n noemen we de *modulus*.
- Bereken $\phi(n) = (p-1)(q-1)$, en kies een getal e met $3 \leq e < \phi(n)$ dat geen delers met $\phi(n)$ gemeen heeft. Deze e noemen we de *publieke exponent*.
- Bereken het getal d, de *privé-exponent* genaamd, met de eigenschap dat

(1) $$\boxed{ed \equiv 1 \pmod{\phi(n)}}.$$

- De publieke sleutel bestaat uit de modulus n en de publieke exponent e, en de privé-sleutel uit de (publieke!) modulus n en de privé-exponent d.

Enkele opmerkingen hierbij:

- De priemgetallen moeten groot genoeg zijn, tenminste 150 cijfers, om factorisatie echt moeilijk te laten zijn. Het is niet moeilijk zulke grote priem-

getallen te maken. Zie [B, par. 8.2], [Ke, par. 13.2] of [W1, par. 3.1, 3.3]. Het is aan te bevelen om p en q evenveel cijfers te laten hebben.

- De methode om e onderling ondeelbaar met $\phi(n)$ te kiezen en om d te berekenen is het *uitgebreide algoritme van Euclides*. Zie [B, par. 3.4], [Ke, par. 7.4, 7.5] of [W1, par. 1.6].
- De getallen p, q en $\phi(n)$ zijn niet meer nodig als de publieke en de privé-sleutel eenmaal berekend zijn. Het is verstandig deze getallen te vernietigen, want de privé-exponent kan er eenvoudig uit berekend worden.
- In plaats van eerst e kiezen en dan d berekenen kun je net zo goed eerst d kiezen, en dan e berekenen zodat (1) geldt.

We gaan er van uit dat n en e publiek bekend zijn, dus ook bij een tegenstander die de privé-sleutel (d.w.z. de privé-exponent d) wil achterhalen. Zo'n tegenstander kan proberen om n in factoren te ontbinden, dan kan zij namelijk $\phi(n)$ uitrekenen en met behulp daarvan kan ze uit e ook d berekenen.

2.2 Versleutelen en ontsleutelen

RSA kan gehele getallen versleutelen als die > 1 en $< n - 1$ zijn. Als m zo'n getal is (de 'klare tekst', die niet in verkeerde handen mag vallen), dan wordt het geheimschrift c (de 'cijfertekst', die iedereen mag zien) berekend met behulp van de publieke sleutel (n, e):

(2) $\boxed{c \equiv m^e \pmod{n}}$.

De eigenaar van de privé-sleutel (n, d) is de enige die het geheimschrift c weer kan terugvertalen naar de klare tekst m. Dit ontsleutelen gaat als volgt:

(3) $\boxed{m \equiv c^d \pmod{n}}$.

Enkele opmerkingen hierbij:

- Als je een leesbare tekst bestaande uit letters een leestekens wilt versleutelen zul je die eerst moeten coderen in een getal, bv. met de ASCII-code. In de praktijk wordt RSA overigens vooral gebruikt voor het versleutelen van sleutels, en dat zijn toch al getallen.
- Er zijn efficiënte technieken om te machtsverheffen modulo n. Zie [B, par. 8.2], [Ke, par. 11.3] of [W1, par. 2.2].
- Er moet natuurlijk gegarandeerd zijn dat ontsleutelen inderdaad het versleutelen ongedaan maakt. Dus de uitkomst van de berekening (3) moet de oorspronkelijke m weer opleveren. Deze garantie wordt gegeven door de Stelling van Euler en het verband (1) tussen e en d. De Stelling van Euler zegt dat $a^{\phi(n)} \equiv 1 \pmod{n}$ (tenzij a en n een deler gemeen hebben,

wat in de praktijk niet zal voorkomen). Uit (1) volgt dan dat er een geheel getal k is met $ed = 1 + k\phi(n)$, en daarmee volgt met (2)

$$c^d \equiv (m^e)^d = m^{ed} = m^{1+k\phi(n)} = m \cdot \left(m^{\phi(n)}\right)^k \equiv m \cdot 1^k = m \pmod{n}.$$

2.3 RSA-CRT

Een veelgebruikte variant van RSA is RSA-CRT. Zie [W1, par. 4.6]. Het idee is om, in plaats van modulo n, afzonderlijk modulo p en modulo q te gaan werken. Dat kan alleen bij het ontsleutelen, omdat alleen de eigenaar van de privé-sleutel beschikt over p en q. Hierbij wordt als privé-sleutel niet d opgeslagen, maar de vijf getallen p, q, d_p, d_q, u, waarbij

$$d_p \equiv d \pmod{p-1}, \quad d_q \equiv d \pmod{q-1}, \quad pu \equiv 1 \pmod{q}.$$

Het optreden van de moduli $p-1$ en $q-1$ in de definities van d_p, d_q komt door de Stelling van Euler, die nu voor priem-moduli gebruikt moet worden, en dan luidt: $a^{p-1} \equiv 1 \pmod{p}$, m.a.w. $\phi(p) = p-1$, en net zo voor q. Ontsleutelen gebeurt dan als volgt:

$$m_p \equiv c^{d_p} \pmod{p}, \quad m_q \equiv c^{d_q} \pmod{q},$$

en $m_p \pmod{p}$, $m_q \pmod{q}$ worden dan gecombineerd tot $m \pmod{n}$, door te berekenen

$$m \equiv m_p + pu(m_q - m_p) \pmod{n}.$$

Merk op dat inderdaad

$$m \equiv m_p \pmod{p}, \quad m \equiv m_p + 1(m_q - m_p) = m_q \pmod{q}.$$

Een algemene stelling die deze reconstructie van m modulo n uit m modulo delers van n beschrijft heet de "Chinese Reststelling"[2].

Het voordeel van RSA-CRT boven gewoon RSA is dat het machtsverheffen met veel kleinere getallen gebeurt (p en q zijn maar half zo lang als n), en dat levert aanzienlijke tijdswinst op, zelfs nu voor één ontsleuteling tweémaal een machtsverheffing moet worden uitgevoerd.

3 Zwakke sleutel: te kleine privé-exponent

3.1 Factoriseren, of raden

Een eerste gedachte is dat de sleutel niet te klein mag zijn. Voor de modulus betekent dat dat die zo groot moet zijn dat bekende factorisatietechnieken

[2] Engels: "Chinese Remainder Theorem", vandaar de naam RSA-CRT.

praktisch onuitvoerbaar zijn. De stand van zaken op dit terrein is dat in januari 2010 bekend werd gemaakt [Kl] dat getallen van 768 bits, dat is 232 cijfers, nu routinematig in factoren kunnen worden ontbonden (hoewel dat bepaald geen kleine klus is). Met een ruime marge genomen betekent dat dat toch ten minste 1024 bits (309 cijfers) cijfers nodig zijn voor de modulus. Voor kritische toepassingen wordt al geruime tijd geadviseerd om 2048 bits te gebruiken.

Ook de privé-exponent mag niet makkelijk te raden zijn. Dat betekent dat deze in ieder geval niet te klein mag zijn, anders zijn alle mogelijkheden gewoon uit te proberen. Een vuistregel is dat het vooralsnog praktisch ondoenlijk is om 2^{80} berekeningen te doen. We gaan er daarom van uit dat $d > 2^{80}$.

3.2 Een benaderingsprobleem

Maar dat is niet genoeg, zo merkte Mike Wiener in 1990 op. Hij zag hoe je d eenvoudig kunt berekenen uit de publieke sleutel als $d < n^{1/4}$. Hoe dat gaat laten we nu zien.

Veronderstel dat $d \approx n^\delta$, met $\delta < \frac{1}{4}$. Uit (1) volgt dat er een gehele k is zodat

(4) $\boxed{ed = 1 + k\phi(n)}$.

Nu is het zo dat als d essentieel kleiner is dan n, het getal e met grote waarschijnlijkheid ongeveer even veel cijfers heeft als n. Omdat

$$\phi(n) = (p-1)(q-1) = n - (p+q) + 1$$

even veel cijfers heeft als n, volgt uit (4) dat k ongeveer even veel cijfers als d zal hebben. We zeggen: ook $k \approx n^\delta$, en $e \approx n$. We kijken nog iets nauwkeuriger naar $\phi(n)$: dit getal ligt zelfs tamelijk dicht bij n, want $n - \phi(n) = p + q - 1$, en p en q hebben beide ongeveer de helft van het aantal cijfers van n, m.a.w. $p, q \approx n^{1/2}$, omdat n immers hun product is.

Uit (4) leiden we nu af:

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \frac{1}{nd}\,|ed - kn| = \frac{1}{nd}\,|1 + k(\phi(n) - n)| \approx \frac{1}{nd}k(p+q),$$

en met de schattingen $d, k \approx n^\delta$ en $p, q \approx n^{1/2}$ vinden we

(5) $\boxed{\left|\frac{e}{n} - \frac{k}{d}\right| \approx n^{-1/2}}$.

De breuk $\frac{e}{n}$ bestaat helemaal uit publieke informatie. De breuk $\frac{k}{d}$ is bij de tegenstander niet bekend, maar we zien hier wel dat deze breuk dicht bij het bekende getal $\frac{e}{n}$ moet liggen. Op zich is dat niet bijzonder, want er zijn heel veel van zulke breuken. Maar de meeste daarvan hebben grote teller en noemer.

Het probleem om benaderingsbreuken $\frac{T}{N}$ te vinden van een gegeven reëel getal α is een klassiek probleem, waarbij de afstand $\left|\alpha - \frac{T}{N}\right|$ afgewogen wordt tegen de grootte van teller en noemer. Als je met breuken $\frac{T}{N}$ steeds dichter bij α wilt komen, zul je steeds grotere tellers en noemers moeten nemen. Dit leidt tot de volgende definitie.

Definitie. *De vereenvoudigde breuk* $\frac{T}{N}$ *wordt* beste benadering *van* α *genoemd als iedere breuk die dichter bij* α *ligt een noemer groter dan* N *heeft.*

3.3 Kettingbreuken

Er is een fraaie manier om de beste benaderingen van een gegeven getal α te vinden. Dat gaat met de kettingbreuk van α. Met de notatie $\lfloor x \rfloor$ bedoelen we het gehele deel van x, oftewel afronden naar beneden.

Laat $a_0 = \lfloor \alpha \rfloor$. Bereken dan $\alpha_1 = \dfrac{1}{\alpha - a_0}$, zodat $\alpha = a_0 + \dfrac{1}{\alpha_1}$. Nu is $\alpha_1 > 1$, en we nemen dan $a_1 = \lfloor \alpha_1 \rfloor$. Bereken dan $\alpha_2 = \dfrac{1}{\alpha_1 - a_1}$, zodat $\alpha = a_0 + \dfrac{1}{a_1 + \frac{1}{\alpha_2}}$.
Zo gaan we door. We krijgen dan de *kettingbreuk* van α: een schrijfwijze van α met behulp van een rij gehele getallen $a_0, a_1, a_2, a_3, \ldots$:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}.$$

Omdat dit een typografische nachtmerrie wordt, is de notatie

$$\alpha = [a_0, a_1, a_2, a_3, \ldots]$$

gebruikelijker. Als α rationaal is, dan zal op een gegeven moment een α_k geheel worden, en dan stopt de kettingbreukontwikkeling. Een voorbeeld:
$\alpha = \dfrac{23}{16} = 1 + \dfrac{7}{16}$, dus $a_0 = 1$, en $\alpha_1 = \dfrac{16}{7} = 2 + \dfrac{2}{7}$, dus $a_1 = 2$, en
$\alpha_2 = \dfrac{7}{2} = 3 + \dfrac{1}{2}$, dus $a_2 = 3$, en $\alpha_3 = \dfrac{2}{1} = 2$, dus $a_3 = 2$, en het proces stopt.
Er volgt $\dfrac{23}{16} = 1 + \dfrac{1}{2 + \frac{1}{3 + \frac{1}{2}}}$, oftewel $\dfrac{23}{16} = [1, 2, 3, 2]$.

Een ander voorbeeld:
$\alpha = \pi = 3.14159\ldots = 3 + 0.14159\ldots$, dus $a_0 = 3$, en
$\alpha_1 = \dfrac{1}{0.14159\ldots} = 7.06251\ldots = 7 + 0.06251\ldots$, dus $a_1 = 7$, en
$\alpha_2 = \dfrac{1}{0.06251\ldots} = 15.99659\ldots = 15 + 0.99659\ldots$, dus $a_2 = 15$, en

$\alpha_3 = \dfrac{1}{0.99659\ldots} = 1.00341\ldots = 1 + 0.00341\ldots$, dus $a_3 = 1$, en

$\alpha_4 = \dfrac{1}{0.00341\ldots} = 292.63459\ldots = 292 + 0.63459\ldots$, dus $a_4 = 292$, enzovoorts.

Er volgt $\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{\ddots}}}}}$, oftewel $\pi = [3, 7, 15, 1, 292, \ldots]$.

Een eindige kettingbreuk levert een rationaal getal op[3]. Bijvoorbeeld, enig rekenen geeft: $[3, 7, 15, 1] = \dfrac{355}{113}$. Het valt op dat $\dfrac{355}{113} = 3.14159292\ldots$ een heel goede benadering van $\pi = 3.14159265\ldots$ is[4]. De theorie van de kettingbreuken verklaart dit. Eerst geven we de breuken die je krijgt door een kettingbreuk ergens af te kappen een naam.

Definitie. *Laat α de kettingbreukontwikkeling $\alpha = [a_0, a_1, a_2, \ldots]$ hebben. Noteer $\dfrac{T_i}{N_i} = [a_0, a_1, a_2, \ldots, a_i]$ voor de achter a_i afgekapte kettingbreuk, met $\dfrac{T_i}{N_i}$ de vereenvoudigde breuk. Deze breuken $\dfrac{T_i}{N_i}$ noemen we* convergenten *van α. De getallen $a_0, a_1, a_2, \ldots$ heten* wijzergetallen *van α.*

De centrale stelling uit de kettingbreuktheorie is de volgende. Zie bijvoorbeeld [B, hst. 14], [Ke, par. 7.6, 15.6, 15.7] voor bewijzen.

Stelling.

(a) *Voor de convergenten $\dfrac{T_i}{N_i}$ van α geldt*

(6) $$\boxed{\frac{1}{(a_{i+1}+2)N_i^2} < \left|\alpha - \frac{T_i}{N_i}\right| < \frac{1}{a_{i+1}N_i^2}}.$$

(b) *Een convergent van α is altijd een beste benadering van α, en andersom: een beste benadering van α is altijd een convergent van α.*

Ongelijkheid (6) doet precies wat we willen: het afwegen van de afstand van de breuk $\dfrac{T_i}{N_i}$ tot α tegen de grootte van de noemer. Een direct gevolg van ongelijkheid (6) is dat $\lim\limits_{i\to\infty} \dfrac{T_i}{N_i} = \alpha$, in woorden: de rij van de convergenten van α convergeert inderdaad naar α.

Een andere interessante observatie op grond van (6) is dat als je een extra groot wijzergetal a_{i+1} tegenkomt, de eraan voorafgaande convergent $\dfrac{T_i}{N_i}$ een

[3] In het rationale geval is overigens het kettingbreukalgoritme essentieel hetzelde als het algoritme van Euclides voor het berekenen van de ggd van teller en noemer.

[4] De Chinees Zu Chongzhi wist dat al in de 5e eeuw. De eerste Europese vermelding is uit 1585, van Adriaan Anthoniszoon. Archimedes (3e eeuw v. Chr.) wist al wel dat $\dfrac{22}{7} = [3, 7]$ een goede benadering van π is.

extra goede benadering van α is. Dat zagen we bij $\frac{355}{113}$ als benadering van π al optreden, kennelijk vanwege het bijzonder grote wijzergetal 292 in de kettingbreuk van π.

Als α tot op voldoende cijfers achter de komma bekend is, zeg tot op b cijfers, dan zijn de convergenten met noemers tot aan ongeveer $b/2$ cijfers heel snel te berekenen. De te gebruiken formules zijn

$$\begin{cases} T_{-2} = 0, & T_{-1} = 1, & T_i = a_i T_{i-1} + T_{i-2} \\ N_{-2} = 1, & N_{-1} = 0, & N_i = a_i N_{i-1} + N_{i-2} \end{cases} \qquad \text{voor } i = 0, 1, 2, \ldots$$

(zie de genoemde literatuur voor de afleiding ervan). Gebruik makend van $a_i \geq 1$ voor $i \geq 1$ is meteen in te zien dat $N_i \geq F_{i+1}$, waarbij F_i het i-e Fibonacci-getal is. Dat impliceert dat de noemers N_i exponentieel hard groeien, want dat doen de Fibonacci-getallen F_i al.

Voor de toepassing is het onderstaande gevolg van deze stelling heel nuttig.

Stelling. *Als* $\frac{T}{N}$ *een breuk is die voldoet aan*

$$\boxed{\left|\alpha - \frac{T}{N}\right| < \frac{1}{2N^2}}, \tag{7}$$

dan is $\frac{T}{N}$ *een convergent van* α.

Bewijs: Laat $\frac{T'}{N'}$ een breuk zijn die dichter bij α ligt dan $\frac{T}{N}$. Dan is

$$\left|\frac{T'}{N'} - \frac{T}{N}\right| \leq \left|\frac{T'}{N'} - \alpha\right| + \left|\alpha - \frac{T}{N}\right| < 2\left|\alpha - \frac{T}{N}\right| < \frac{1}{N^2},$$

en omdat $T'N - TN'$ geheel is en niet 0, volgt

$$1 \leq |T'N - TN'| = NN'\left|\frac{T'}{N'} - \frac{T}{N}\right| < NN'\frac{1}{N^2} = \frac{N'}{N}.$$

Hier staat dat $N' > N$, dus iedere breuk die dichter bij α ligt dan $\frac{T}{N}$ heeft een grotere noemer. Dus is $\frac{T}{N}$ een beste benadering van α, dus een convergent. □

3.4 Het kraken

Nu gaan we deze theorie toepassen op ons probleem om de privé-exponent d te achterhalen als deze erg klein is. Dan hebben we uitdrukking (5), en hierbij is $\alpha = \frac{e}{n}$ bekend. Ongelijkheid (7) met $\frac{T}{N} = \frac{k}{d}$ zegt dat $\frac{k}{d}$ een convergent is als

$n^{-1/2} < \frac{1}{2d^2}$. Als we de factor 2 voor het gemak even verwaarlozen (we zijn op wel meer plekken een beetje slordig geweest in de afschattingen), dan zien we dat dit het geval is als $d < n^{1/4}$, dus als $\delta < 1/4$. Dat betekent dan dat we alleen maar de convergenten van de kettingbreuk van $\frac{e}{n}$ hoeven uit te rekenen tot de noemers groter worden dan $n^{1/4}$. Dat zijn er maar een paar, want ze groeien exponentieel. Die kandidaten voor $\frac{k}{d}$ testen we dan of ze voldoen. En mocht δ echt een stukje kleiner zijn dan $\frac{1}{4}$, dan zegt (6) bovendien dat we een extreem groot wijzergetal zullen tegenkomen, en weten we doorgaans meteen welke convergent we moeten hebben.

3.5 Een voorbeeld

U zult begrijpen dat we geen voorbeeld nemen met een modulus van 300 cijfers, maar een veel kleinere. Voor de methode maakt dat niet uit, voor de rekentijd wel, maar met moderne computers en de juiste software blijft het binnen een fractie van een seconde.

Laten we $n = 20532004352107574659 2613$ en $e = 70760135995620281241019$ nemen. Stel we vermoeden dat de bijbehorende d echt een stukje kleiner dan $n^{1/4}$ gekozen was. Dan berekenen we de kettingbreuk van $\frac{e}{n}$, deze blijkt te beginnen als $[0, 2, 1, 9, 6, 54, 5911, 1, 5, 1, 1, \ldots]$. Het grote wijzergetal 5911 suggereert om $\frac{k}{d} = [0, 2, 1, 9, 6, 54]$ uit te proberen, dat is $k = 3304$, $d = 9587$. Dat uittesten van een kandidaat $\frac{k}{d}$ gaat als volgt: in de gelijkheid (4) weten we nu alle getallen behalve $\phi(n)$, en die kunnen we er dus uit oplossen:

$$\begin{aligned}\phi(n) = \frac{ed-1}{k} &= (70760135995620281241019 \cdot 9587 - 1)/3304 \\ &= 205320043519979308794688.\end{aligned}$$

Dit is een geheel getal, en dat zegt op zich al iets, want bij 'verkeerde' convergenten zal hier vaak een niet-geheel getal uitkomen. Nu weten we

$$p + q = n + 1 - \phi(n) = 1096437797926,$$

en ook wisten we

$$pq = n = 205320043521075746592613.$$

Uit deze twee vergelijkingen kunnen we (met de *abc*-formule) kijken of we gehele p en q vinden. Dat gaat inderdaad goed: $p = 239635170197$ en $q = 856802627729$, en deze kloppen.

3.6 Priemfactoren dicht bij elkaar

We gaan nog iets nauwkeuriger kijken naar n als benadering van $\phi(n)$. De fout $n - \phi(n)$ is immers de term die in (5) de hoofdverantwoordelijke is voor de afschatting $n^{-1/2}$. Dit kunnen we ietsje beter doen, door niet n maar $n+1-2\sqrt{n}$ te nemen als benadering van $\phi(n)$, en dus niet de kettingbreuk van $\frac{e}{n}$ te bekijken, maar die van $\frac{e}{n+1-2\sqrt{n}}$. Immers,

$$n+1-2\sqrt{n}-\phi(n) = p+q-2\sqrt{pq} = (\sqrt{p}-\sqrt{q})^2 = \frac{(p-q)^2}{\left(\sqrt{p}+\sqrt{q}\right)^2} \approx \frac{(p-q)^2}{4\sqrt{n}}.$$

Deze afschatting komt in de plaats van $n - \phi(n) = p + q - 1 \approx 2\sqrt{n}$. En in plaats van (5) vinden we nu

$$\left|\frac{e}{n+1-2\sqrt{n}} - \frac{k}{d}\right| \approx \frac{(p-q)^2}{n^{3/2}}.$$

Als p en q dicht bij elkaar liggen, zeg $|p-q| \approx n^\beta$ voor een $\frac{1}{4} < \beta < \frac{1}{2}$, betekent dit dat de eis van $d > n^{1/4}$ navenant verscherpt zal moeten worden tot $d > n^{3/4-\beta}$ (als $\beta \leq \frac{1}{4}$ dan is er een veel simpeler methode, zie [W2, deel 1]). Als de priemgetallen onafhankelijk van elkaar willekeurig worden gekozen is de kans dat dit optreedt overigens astronomisch klein.

4 Zwakke sleutel: te kleine privé-exponent - geavanceerd

4.1 Een polynoom met een klein nulpunt

Je kunt je afvragen waarom je eigenlijk een kleine privé-exponent zou willen: kun je hem niet altijd gewoon groot nemen? Ja, dat kan. Maar een kleine exponent kan wel voordelen hebben. De rekentijd van een machtsverheffing modulo n hangt sterk af van de grootte van de exponent: afhankelijk van de implementatie kan de rekentijd omhoog gaan met de derde macht van het aantal cijfers van de exponent. Als je het ontsleutelen op een langzame (want goedkope) processor als die van een smartcard moet doen, kan een kleine privé-exponent d dus best nuttig zijn. Hier is dus na Wiener's resultaat meer onderzoek naar gedaan. Daar is uitgekomen dat je nog meer moet oppassen: zelfs voor $\delta < 0.292$ (dus $d < n^{0.292}$) blijkt RSA onveilig te zijn. We zullen de gebruikte techniek aan de hand van een voorbeeld illustreren. Dit is werk van Dan Boneh en Glenn Durfee uit 2000, gebaseerd op ideeën van Don Coppersmith.

We nemen dezelfde n, e als in paragraaf 3.5: $n = 20532004352107574659261 3$ en $e = 70760135995620281241019$. Dat de bijbehorende d al gevonden was moet

u even vergeten. Het gaat erom dat we diezelfde d nu met een heel andere techniek ook kunnen vinden. Dat die nieuwe techniek ook voor grotere d dan $n^{1/4}$ werkt is aangetoond, maar dat kunnen we nu niet laten zien.

Kijk weer naar vergelijking (4), en wel in de vorm

$$ed = 1 + k(n + 1 - (p + q)).$$

Deze vergelijking nemen we nu modulo e. Het prettige daarvan is dat de onbekende d dan opeens er niet meer toe doet. De onbekenden zijn nu k en $p + q$, en die zijn samen een nulpunt $\pmod e$ van het polynoom

$$\boxed{f(x, y) = xy - (n + 1)x - 1},$$

want $f(k, p + q) \equiv 0 \pmod e$. Wat hierbij prettig is is dat zowel k als $p + q$ relatief klein zijn t.o.v. de grootste coëfficiënt van het polynoom f. In ons voorbeeld nemen we als bovengrens voor k nu $X = 10^4$, en als bovengrens voor $p + q$ nemen we $Y = 10^{12}$.

Het idee van Don Coppersmith was nu tweeledig:

- als een polynoom $g(x, y)$ een nulpunt $(x_0, y_0) \pmod M$ heeft, dus M is een deler van $g(x_0, y_0)$, en $g(x, y)$ heeft *zulke kleine* coëfficiënten en het nulpunt (x_0, y_0) is *zo klein* t.o.v. de *zo grote* modulus M dat $|g(x_0, y_0)| < M$ waar blijkt te zijn, dan moet (x_0, y_0) dus *zelfs zonder de modulus* al een nulpunt van $g(x, y)$ zijn, oftewel dan is $g(x_0, y_0) = 0$;
- er zijn trucs om uit een polynoom $f(x, y)$ met *grote* coëfficiënten een polynoom met *kleinere* coëfficiënten te maken dat *hetzelfde nulpunt* $\pmod M$ heeft.

Het eerste idee kan precies gemaakt worden. De volgende stelling is een speciaal geval van een resultaat van Nick Howgrave-Graham.

Stelling (Howgrave-Graham). *Laat $h(x, y)$ een polynoom zijn met maximaal 4 termen en gehele coëfficiënten. Laat de gehele getallen x_0, y_0 voldoen aan $h(x_0, y_0) \equiv 0 \pmod M$, en aan $|x_0| \leq X$, $|y_0| \leq Y$, voor zekere gegeven M, X, Y. Als nu alle coëfficiënten van $h(xX, yY)$ in absolute waarde $< \frac{1}{2}M$ zijn, dan is $h(x_0, y_0) = 0$.*

Bewijs: Laat $h(x, y) = \sum b_{i,j} x^i y^j$. De coëfficiënten van $h(xX, yY)$ zijn dan $b_{i,j} X^i Y^j$, en dus

$$\begin{aligned} |h(x_0, y_0)| &= \left|\sum b_{i,j} x_0^i y_0^j\right| \leq \sqrt{\sum \left(b_{i,j} x_0^i y_0^j\right)^2} \\ &= \sqrt{\sum \left(b_{i,j} X^i Y^j\right)^2 \left(\frac{x_0}{X}\right)^{2i} \left(\frac{y_0}{Y}\right)^{2j}} < \sqrt{4 \cdot \left(\tfrac{1}{2}M\right)^2} = M, \end{aligned}$$

en omdat $h(x_0, y_0)$ geheel is, en deelbaar door M, moet het wel 0 zijn. □

4.2 Polynomen met kleine coëfficiënten

Voor het tweede idee van Coppersmith zijn verschillende strategieën bedacht. Die kunnen we hier niet behandelen. Zie [H] en [J] voor een overzicht. Aan de hand van ons concrete voorbeeld kunnen we wel een idee geven hoe het werkt.

Als modulus kiezen we $M = e^2$, en we gaan eerst maar eens een aantal polynomen opschrijven waarvan we zeker weten dat $(x_0, y_0) = (k, p+q)$ een nulpunt van $f(x,y) \pmod{e^2}$ is, zonder dat we k en $p+q$ kennen. Namelijk:

$$\begin{array}{l|l|l} g_{0,0}(x,y) = e^2 & g_{2,0}(x,y) = e^2x^2 & h_{1,0}(x,y) = e^2y \\ g_{1,0}(x,y) = e^2x & g_{1,1}(x,y) = e\ x\ f(x,y) & h_{1,1}(x,y) = e\ yf(x,y) \\ g_{0,1}(x,y) = e\quad f(x,y) & g_{0,2}(x,y) = \quad f(x,y)^2 & h_{1,2}(x,y) = \quad yf(x,y)^2 \end{array}$$

De volgende tabel bevat de coëfficiënten van deze polynomen:

	1	x	xy	x^2	x^2y	x^2y^2	y	xy^2	x^2y^3
$g_{0,0}$	e^2								
$g_{1,0}$		e^2							
$g_{0,1}$	$-e$	$-e(n+1)$	e						
$g_{2,0}$				e^2					
$g_{1,1}$		$-e$		$-e(n+1)$	e				
$g_{0,2}$	1	$2(n+1)$	-2	$(n+1)^2$	$-2(n+1)$	1			
$h_{1,0}$							e^2		
$h_{1,1}$			$-e(n+1)$				$-e$	e	
$h_{1,2}$			$2(n+1)$		$(n+1)^2$	$-2(n+1)$		-2	1

Deze polynomen zijn natuurlijk niet zomaar gekozen, daar zit een strategie achter, die o.a. tot de bovenstaande driehoekige vorm leidt.

Het idee is nu om lineaire combinaties van deze polynomen te kiezen, zodat de coëfficiënten zo klein mogelijk worden. De theorie hierachter is die van *roosterbasisreductie*, en het algoritme dat dit efficiënt doet is het zogenaamde LLL-algoritme. Dat kan gezien worden als een generalisatie van het algoritme van Euclides. We gaan niet op de details in, maar vermelden het resultaat: we vinden o.a.

$$\begin{aligned} p_1(x,y) &= 91910569g_{2,0}(x,y) + 63350896g_{1,1}(x,y) + 10916416g_{0,2}(x,y) \\ &= 10916416 + 23938342240568299824x \\ &\quad + 131234516261238241782836623350 09x^2 - 21832832xy \\ &\quad - 23938342240568299824x^2y + 10916416x^2y^2, \\ p_2(x,y) &= -964355g_{1,0}(x,y) - 332346g_{0,1}(x,y) \\ &\quad + 17286884292171605419691 79g_{2,0}(x,y) \\ &\quad + 17872910931668028426742 68g_{1,1}(x,y) \\ &\quad + 41064008704642407047419 6g_{0,2}(x,y) + h_{1,2} \\ &= 23517258797687464413398174770 \\ &\quad - 21457461892318384535056334741370599284123x \\ &\quad + 35649776482295032433498368412689403 47x^2 + y \\ &\quad - 23517258797687468685975463738xy \\ &\quad + 39027768456154986743754 00x^2y - 2xy^2 + 4272577288968x^2y^2 + x^2y^3. \end{aligned}$$

Duidelijk is dat inderdaad $p_1(x_0, y_0) \equiv p_2(x_0, y_0) \equiv 0 \pmod{e^2}$. De grootste coëfficiënt van $p_1(xX, yY)$ is $2.393\ldots\cdot 10^{39}$, die van $p_2(xX, yY)$ is $4.272\ldots\cdot 10^{44}$, en die zijn inderdaad kleiner dan $\frac{1}{2}e^2 = 2.503\ldots\cdot 10^{45}$. Dus weten we nu op grond van de stelling van Howgrave-Graham dat $x_0 = k$ en $y_0 = p + q$ van beide polynomen echte nulpunten zijn: $p_1(x_0, y_0) = p_2(x_0, y_0) = 0$.

4.3 Het vinden van het nulpunt

Maar hoe vinden we daaruit de waarden van x_0 en y_0?

Wat we doen is polynomen $a_1(x, y), a_2(x, y)$ zoeken zodat uit $a_1p_1 + a_2p_2$ de variabele x helemaal verdwenen is. Dat is niet zo heel moeilijk. De algemene methode is het berekenen van een zogenaamde *resultante* van p_1 en p_2. In dit geval gaat dat als volgt (in feite ook weer een generalisatie van het algoritme van Euclides). Schrijven we

$$p_1(x, y) = b_1(y) + c_1(y)x + d_1(y)x^2, \quad p_2(x, y) = b_2(y) + c_2(y)x + d_2(y)x^2,$$

dan zien we dat $p_3 = d_1p_2 - d_2p_1$ alvast geen x^2 meer bevat. En op dezelfde manier is een combinatie p_4 van p_2 en xp_3 te vinden die ook geen x^2 meer bevat. Tenslotte is op dezelfde manier een combinatie p_5 van p_3 en p_4 te vinden die ook geen x meer bevat. Het blijkt dat

$$\begin{aligned} a_1 &= -d_2(b_1d_2 - b_2d_1) + (c_2 + d_2x)(c_1d_2 - c_2d_1), \\ a_2 &= d_1(b_1d_2 - b_2d_1) - (c_1 + d_1x)(c_1d_2 - c_2d_1) \end{aligned}$$

leidt tot:

$$p_5 = a_1p_1 + a_2p_2 = (c_1d_2 - c_2d_1)(b_1c_2 - b_2c_1) - (b_1d_2 - b_2d_1)^2,$$

een uitdrukking die nog steeds hetzelfde nulpunt heeft, maar niet meer van x afhangt, alleen nog van y. Hier is dat

$$\begin{aligned} p_5(y) = a_1(x, y)p_1(x, y) + a_2(x, y)p_2(x, y) &= 45186470870881861783781526386044\backslash \\ &\quad 84590883818561242978066441050834049358921519373818309427961837356 \\ &\quad - 82424139255971828392316121222520171443544911347248067754516954088 82\backslash \\ &\quad 778504226715144612y + 375872390626644283990611096324048907 2\backslash \\ &\quad 5078652939629028362425135941 31y^2. \end{aligned}$$

Dit polynoom heeft uiteraard y_0 als nulpunt. Het nulpunt vinden van een polynoom van slechts één variabele is kinderspel. Hier hebben we een kwadratisch polynoom, en zouden we de *abc*-formule kunnen gebruiken. Maar ook numerieke nulpuntzoekmethoden zijn bruikbaar. Hoe dan ook, hier vinden we

$$\begin{aligned} p_5(y) &= 375872390626644283990611096324048907283023250786529396290283624\backslash \\ &\quad 2513594131 \cdot (-1096437797926 + y)^2, \end{aligned}$$

en we zien dat $y_0 = p + q = 1096437797926$. Dat geeft voldoende informatie (samen met $pq = n = 205320043521075746592613$) om p en q te berekenen. En dan is het vinden van d niet moeilijk meer.

Al deze berekeningen lijken erg ingewikkeld, door de erg grote getallen die er optreden. Maar daar moet u even doorheen prikken. In de praktijk wil je deze berekeningen doen met veel grotere getallen (bijv. n van zo'n 300 cijfers). Met een computer-algebra-pakket als Mathematica is dat niet moeilijker dan rekenen met getallen van 3 cijfers. De methode blijft exact hetzelfde, de optredende polynomen hebben dezelfde vorm, alleen grotere coëfficiënten.

5 Gedeeltelijk gelekte sleutel: factoriseren met een hint

5.1 Een polynoom met een klein nulpunt

Onder bepaalde omstandigheden kunnen delen van privé-sleutels lekken. Een techniek daarvoor is het nauwkeurig meten van het stroomgebruik van een smartcard op het moment dat die bezig is met een berekening met die privé-sleutel. Bijvoorbeeld, het programma zal wellicht iets meer werk moeten doen voor het verwerken van een bit dat 1 is dan voor een 0, en dan iets meer stroom verbruiken.

Het is o.a. daarom interessant geworden om te kijken hoeveel van de privé-sleutel moet lekken om de rest te kunnen berekenen. De techniek die behandeld is in hoofdstuk 4 kan worden aangepast voor het geval dat de privé-exponent niet klein is, maar voor een deel bekend.

We zullen nu echter een wat ander voorbeeld bekijken, waarin een dergelijke techniek wordt gebruikt om $n = pq$ in factoren te ontbinden als van de priemfactoren p en q het nodige gelekt is. De techniek werkt in principe als de bovenste helft van de cijfers van p bekend is (en dus ook van q), of de onderste helft. We demonstreren de techniek nu aan dezelfde $n = 20532004352107574659261 3$ als hierboven, waarbij we als extra informatie (de 'hint') hebben dat 2396352 de bovenste 7 (van de 12) cijfers van p zijn, en 8568026 die van q.

We schrijven $p = p_0 + x_0$, $q = q_0 + y_0$, met $p_0 = 239635200000$, $q_0 = 856802600000$, en x_0, y_0 onbekend met beide $|x_0|, |y_0| < X = 10^5$. Nu is (x_0, y_0) een klein nulpunt van het polynoom

$$\boxed{f^*(x,y) = (p_0 + x)(q_0 + y) - n = (p_0 q_0 - n) + q_0 x + p_0 y + xy}.$$

Om technische redenen willen we graag een polynoom met constante term 1. We nemen nu een modulus $M = 10^{37}$, en berekenen c zodanig dat $c(p_0 q_0 - n) \equiv 1 \pmod{M}$, en $a \equiv cq_0 \pmod{M}$, $b = cp_0 \pmod{M}$. Dat geeft

$$\begin{aligned} c &= 47735829292983994054711929151687223 23, \\ a &= 84847864461723148181407250244398000 00, \\ b &= 90078012099704084650398076165696000 00. \end{aligned}$$

Nu nemen we

$$\boxed{f(x,y) = 1 + ax + by + cxy},$$

want $f(x_0, y_0) \equiv cf^*(x_0, y_0) = 0 \pmod{M}$.

5.2 Polynomen met kleine coëfficiënten

De strategie om een aantal polynomen op te schrijven waarvan we zeker weten dat (x_0, y_0) een nulpunt (mod M) is, geeft nu:

$$\begin{array}{l|l|l} g_{0,0}(x,y) = X^4 \ f(x,y) & g_{1,1}(x,y) = X^2xyf(x,y) & h_{2,1}(x,y) = Mx^2y \\ g_{1,0}(x,y) = X^3xf(x,y) & h_{2,0}(x,y) = M\ x^2 & h_{1,2}(x,y) = Mxy^2 \\ g_{0,1}(x,y) = X^3yf(x,y) & h_{0,2}(x,y) = M\ y^2 & h_{2,2}(x,y) = Mx^2y^2 \end{array}$$

De volgende tabel bevat de coëfficiënten van deze polynomen:

	1	x	y	xy	x^2	y^2	x^2y	xy^2	x^2y^2
$g_{0,0}$	X^4	aX^4	bX^4	cX^4					
$g_{1,0}$		X^3		bX^3	aX^3		cX^3		
$g_{0,1}$			X^3	aX^3		bX^3		cX^3	
$g_{1,1}$				X^2			aX^2	bX^2	cX^2
$h_{2,0}$					M				
$h_{0,2}$						M			
$h_{2,1}$							M		
$h_{1,2}$								M	
$h_{2,2}$									M

De techniek van roosterbasisreductie geeft nu een aantal polynomen met kleine coëfficiënten die lineaire combinaties zijn van bovenstaande, we selecteren daar één uit:

$$\begin{aligned} p(x,y) = {} & 34853558839845024g_{0,0}(x,y) \\ & - 29572500364518632902878965837831683033644466122567946256727g_{1,0}(x,y) \\ & - 31395392948933083309478264368411070333007955918672712382199g_{0,1}(x,y) \\ & + 532766409130722573703404011658772635302398388736552492803890068499\backslash \\ & \quad 0378624300023586334019218741289240582248002009_{1,1}(x,y) \\ & + 250916350272293535791075636442142577931629039003557032048099531774\backslash \\ & \quad 86609166h_{2,0}(x,y) \\ & + 28280345859289585817611178346362583484505908334310306340972059243\backslash \\ & \quad 462400717h_{0,2}(x,y) \\ & - 45204092071682490824457259466261991011752205482200501124149230054\backslash \\ & \quad 36238477602280830676256289704990531710269405 9h_{2,1}(x,y) \\ & - 47990539047993124717584289016595503364691998143993633257014623840\backslash \\ & \quad 12698251776302060074511213973073318070430763h_{1,2}(x,y) \\ & - 25432046359300241870051436398798758002499757236143986334379471470\backslash \\ & \quad 72717089990151413665218230648585147806835489h_{2,2}(x,y) \\ = {} & 34853558839845024000000000000000000000 \\ & - 24367047946256727000000000000000x - 1565346000000000000000000000x^2 \\ & - 10495163271238219900000000000000y + 19817767412892405822480020 0xy \\ & - 70104735280720400000000x^2y - 48455040000000000000000000y^2 \\ & + 23503326169393920000000xy^2 + 12485854595486460 0x^2y^2 \end{aligned}$$

Nu is weer duidelijk dat inderdaad $p(x_0, y_0) \equiv 0 \pmod{M}$. De grootste coëfficiënt van $p(xX, yX)$ is $2.350\ldots \cdot 10^{37}$, en die is weliswaar net ietsje groter dan $\frac{1}{2}M = 5.000\ldots \cdot 10^{36}$, zodat aan de voorwaarden van de stelling van Howgrave-Graham niet is voldaan, maar toch blijkt dit polynoom te werken.

5.3 Het vinden van het nulpunt

De reden dat we nu maar één polynoom p hoeven te selecteren, is dat we al een ander polynoom hebben waarvan we zeker weten dat (x_0, y_0) een echt (niet-modulair) nulpunt is, namelijk f^*. We kunnen nu weer een lineaire combinatie van p en f^* zoeken die niet meer van x afhangt. Dat is hier ietsje simpeler dan in paragraaf 4.3, omdat één van de twee polynomen nu geen x^2 heeft. We schrijven dus

$$p(x, y) = b_1(y) + c_1(y)x + d_1(y)x^2, \quad f^*(x, y) = b_2(y) + c_2(y)x,$$

dan zien we dat $p_1 = d_1 x f^* - c_2 p$ geen x^2 meer bevat. De juiste combinatie p_2 van p_1 en f^* bevat dan ook geen x meer. Het blijkt dat

$$a_1 = -c_2^2, \quad a_2 = c_2 d_1 x - (b_2 d_1 - c_1 c_2)$$

leidt tot:

$$p_2 = a_1 p + a_2 f^* = c_2(b_2 c_1 - b_1 c_2) - b_2^2 d_1,$$

een uitdrukking die nog steeds hetzelfde nulpunt heeft, maar niet meer van x afhangt, alleen nog van y. Hier is dat

$$\begin{aligned} p_2(y) &= a_1(x, y)p(x, y) + a_2(x, y)f^*(x, y) \\ &= 10000000000000000000000000000000000000000 \cdot (28971678074274940917065 4 \\ &\quad - 79169533269942837 71y - 80471757777041y^2 - 409785919y^3 + 717y^4). \end{aligned}$$

Dit polynoom heeft $y_0 = 27729$ als nulpunt. Daarmee hebben we $q = q_0 + y_0 = 856802627729$ gevonden, en volgt meteen $p = n/q = 239635170197$, en is n in factoren ontbonden.

6 Mishandelde sleutel: de magnetron-aanval

6.1 Smartcard in de magnetron

Tenslotte beschrijven we een heel ander soort aanval op RSA. We gaan uit van de situatie dat de tegenstander een smartcard in handen heeft gekregen, die zij berekeningen kan laten doen met de privé-sleutel. Met andere woorden, als zij aan de smartcard een geheimschrift c aanbiedt, dan geeft de smartcard het ontsleutelde getal $c^d \pmod{n}$ terug, maar zonder informatie over de privé-sleutel te lekken. De tegenstander wil de privé-sleutel achterhalen. We gaan er

ook van uit dat de privé-sleutel in CRT-vorm op de smartcard ligt opgeslagen, dus de getallen p, q, d_p, d_q, u zoals in paragraaf 2.3 beschreven.

De tegenstander legt de smartcard even in de magnetron. De straling zal de inhoud van het geheugen op de chip kunnen beschadigen. We gaan er van uit dat die beschadiging alléén optreedt in het veld waar, bijvoorbeeld, d_p zich bevindt. Na de mishandeling bevat de smartcard dan d'_p in plaats van d_p, maar alle andere getallen, p, q, d_q, u, zijn nog intact.

6.2 Foute ontsleuteling lekt de sleutel

De tegenstander kiest nu een willekeurig getal m, en versleutelt dit (niet op de smartcard, maar gewoon op een PC) met de publieke sleutel tot $c \equiv m^e \pmod{n}$. Dan biedt zij c aan aan de mishandelde smartcard. Die zal nu een getal m' berekenen, als volgt:

$$m'_p \equiv c^{d'_p} \pmod{p}, \quad m_q \equiv c^{d_q} \pmod{q},$$

$$m' \equiv m'_p + pu(m_q - m'_p) \pmod{n}.$$

Alléén dit getal m' zal de smartcard teruggeven, niet de tussenresultaten of de gebruikte priemgetallen. Merk nu op dat $m' \equiv m'_p \pmod{p}$ in plaats van $m \equiv m_p \pmod{p}$, terwijl $m' \equiv m'_p + 1(m_q - m'_p) = m_q \pmod{q}$ nog wel goed is. Dus

$$m' \not\equiv m \pmod{p}, \quad m' \equiv m \pmod{q}.$$

Maar dat betekent dat $m' - m$ wel deelbaar is door q, maar niet door p. En dan is q eenvoudig te berekenen als $\text{ggd}(m' - m, n)$, en is RSA gekraakt.

6.3 Een voorbeeld

Laat $p = 97, q = 127$, dus $n = 12319$. We nemen $e = 19$, dan is $d_p = 91, d_q = 73, u = 55$. Met $m = 3507$ krijgen we $c \equiv 3507^{19} \equiv 10497 \pmod{12319}$, en een correcte ontsleuteling van c zou op de smartcard zo gaan:

$$m_p \equiv 10497^{91} \equiv 15 \pmod{97}, \quad m_q \equiv 10497^{73} \equiv 78 \pmod{127},$$

$$m \equiv 15 + 97 \cdot 55 \cdot (78 - 15) \equiv 3507 \pmod{12319}.$$

Maar stel nu dat $d_p = 91$ was veranderd in $d'_p = 90$, maar één bitje verschil. Dan zou de smartcard berekend hebben:

$$m'_p \equiv 10497^{90} \equiv 70 \pmod{97}, \quad m_q \equiv 10497^{73} \equiv 78 \pmod{127},$$

$$m' \equiv 70 + 97 \cdot 55 \cdot (78 - 70) \equiv 5793 \pmod{12319}.$$

De tegenstander ziet dat dit niet gelijk is aan $m = 3507$. Nu berekent zij

$$\text{ggd}(5793 - 3507, 12319) = \text{ggd}(2286, 12319) = 127,$$

en heeft ze een priemfactor van n gevonden, en daarmee de beschikking over de volledige privé-sleutel gekregen.

7 Tenslotte

In de standaard-tekstboeken over RSA wordt vaak uitgebreid de moeilijkheid van het factoriseren van grote getallen besproken, en maar weinig tot geen aandacht gegeven aan andere manieren om RSA te kraken. Dat is ook wel te begrijpen, want de methoden die we hierboven besproken hebben werken alleen in heel specifieke omstandigheden. Een te kleine privé-exponent is makkelijk te vermijden. De nuttige efficiëntiewinst kan ook wel op andere manieren behaald worden, bijvoorbeeld door RSA-CRT te gebruiken, in combinatie met een kleine publieke exponent e. In de praktijk wordt vaak $e = 65537$ genomen, erg klein dus, zonder verlies van veiligheid. En smartcards zijn goed te beveiligen tegen het laten lekken van sleutels door stroommetingen of door fouten in de opgeslagen sleutels. Niettemin tonen deze methoden aan dat je er bij het veilig toepassen van RSA niet bent door de modulus maar groot genoeg te kiezen. Het terrein van de cryptanalyse van RSA is de afgelopen 20 jaar een vruchtbaar onderzoeksterrein geweest, ook in Nederland, zoals o.m. blijkt uit het proefschrift [J] van Ellen Jochemsz.

Referenties

[B] Frits Beukers, *Getaltheorie voor beginners*, Epsilon Uitgaven, deel 42, 4e druk, 2008.

[H] M. Jason Hinek, *Cryptanalysis of RSA and its variants*, CRC Press, 2009.

[J] Ellen Jochemsz, *Cryptanalysis of RSA variants using small roots of polynomials*, Proefschrift, TU Eindhoven, 2007.

[Ke] Frans Keune, *Getallen – van natuurlijk naar imaginair*, Epsilon Uitgaven, deel 65, 2009.

[Kl] Thorsten Kleinjung et al., *Factorization of a 768-bit RSA modulus*, Cryptology ePrint Archive, Report 2010/006, `http://eprint.iacr.org/2010/006.pdf`.

[T] Lenny Taelman, *RSA*, in: *Wiskunde en profil – Het gezicht van de wiskunde*, Vakantiecursus 2008, CWI Syllabus 58, 2008, blz. 67–74.

[W1] Benne de Weger, *Elementaire getaltheorie en asymmetrische cryptografie*, Epsilon Uitgaven, deel 63, 2009, bijbehorende educatieve software op `http://www.win.tue.nl/~bdeweger/MCR/`.

[W2] Benne de Weger, *Zwakke sleutels bij het RSA-cryptosysteem*, Euclides 84, no. 7, juni 2009, blz. 256–260, en no. 8, juli 2009, blz. 306–309.

CWI SYLLABI

1. Vakantiecursus 1984: *Hewet - plus wiskunde*. 1984.
2. E.M. DE JAGER, H.G.J. PIJLS (eds.). *Proceedings Seminar 1981–1982. Mathematical structures in fieldtheories*. 1984.
3. W.C.M. KALLENBERG, ET AL. *Testing statistical hypotheses: worked solutions*. 1984.
4. J.G. VERWER (ed.). *Colloquium topics in applied numerical analysis*, volume 1. 1984.
5. J.G. VERWER (ed.). *Colloquium topics in applied numerical analysis*, volume 2. 1984.
6. P.J.M. BONGAARTS, J.N. BUUR, E.A. DE KERF, R. MARTINI, H.G.J. PIJLS, J.W. DE ROEVER. *Proceedings Seminar 1982–1983. Mathematical structures in field theories*. 1985.
7. Vacantiecurus 1985: *Variatierekening*. 1985.
8. G.M. Tuynman. *Proceedings Seminar 1983–1985. Mathematical structures in field theories*, Vol.1 *Geometric quantization*. 1985.
9. J. VAN LEEUWEN, J.K. LENSTRA (eds.). *Parallel computers and computations*. 1985.
10. Vakantiecursus 1986: *Matrices*. 1986.
11. P.W.H. LEMMENS. *Discrete wiskunde: tellen, grafen, spelen en codes*. 1986.
12. J. van de Lune. *An introduction to Tauberian theory: from Tauber to Wiener*. 1986.
13. G.M. TUYNMAN, M.J. BERGVELT, A.P.E. TEN KROODE. *Proceedings Seminar 1983–1985. Mathematical structures in field theories*, Vol.2. 1987.
14. Vakantiecursus 1987: *De personal computer en de wiskunde op school*. 1987.
15. Vacantiecursus 1983: *Complexe getallen*. 1987.
16. P.J.M. Bongaarts, E.A. de Kerf, P.H.M. Kersten. *Proceedings Seminar 1984–1986. Mathematical structures in field theories*, Vol.1. 1988.
17. F. DEN HOLLANDER, H. MAASSEN (eds.). *Mark Kac seminar on probability and physics. Syllabus 1985–1987*. 1988.
18. Vakantiecursus 1988. *Differentierekening*. 1988.
19. R. DE BRUIN, C.G. VAN DER LAAN, J. LUYTEN, H.F. VOGT. *Publiceren met LATEX*. 1988.
20. R. VAN DER HORST, R.D. GILL (eds.). *STATAL: statistical procedures in Algol 60*, part 1. 1988.
21. R. VAN DER HORST, R.D. GILL (eds.). *STATAL: statistical procedures in Algol 60*, part 2. 1988.
22. R. VAN DER HORST, R.D. GILL (eds.). *STATAL: statistical procedures in Algol 60*, part 3. 1988.
23. J. VAN MILL, G.Y. NIEUWLAND (eds.). *Proceedings van het symposium wiskunde en de computer*. 1989.
24. P.W.H. LEMMENS (red.). *Bewijzen in de wiskunde*. 1989.
25. Vakantiecursus 1989: *Wiskunde in de Gouden Eeuw*. 1989.
26. G.G.A. BÄUERLE ET AL. *Proceedings Seminar 1986–1987. Mathematical structures in field theories*. 1990.
27. Vakantiecursus 1990: *Getallentheorie en haar toepassingen*.1990.
28. Vakantiecursus 1991: *Meetkundige structuren*. 1991.
29. A.G. VAN ASCH, F. VAN DER BLIJ. *Hoeken en hun Maat*. 1992.
30. M.J. BERGVELT, A.P.E. TEN KROODE. *Proceedings seminar 1986–1987. Lectures on Kac-Moody algebras*. 1992.
31. Vakantiecursus 1992: *Systeemtheorie*. 1992.
32. F. DEN HOLLANDER, H. MAASSEN (eds.). *Mark Kac seminar on probability and physics. Syllabus 1987–1992*. 1992.
33. P.W.H. LEMMENS (ed.). *Meetkunde van kunst tot kunde, vroeger en nu*. 1993.
34. J.H. KRUIZINGA. *Toegepaste wiskunde op een PC*. 1992.
35. Vakantiecursus 1993: *Het reële getal*. 1993.
36. Vakantiecursus 1994: *Computeralgebra*. 1994.
37. G. ALBERTS. *Wiskunde en praktijk in historisch perspectief*. 1994.
38. G. ALBERTS, J. SCHUT (eds.). *Wiskunde en praktijk in historisch perspectief. Reader*. 1994.
39. E.A. DE KERF, H.G.J. PIJLS (eds.). *Proceedings Seminar 1989–1990. Mathematical structures in field theory*. 1996.
40. Vakantiecursus 1995: *Kegelsneden en kwadratische vormen*. 1995.
41. Vakantiecursus 1996: *Chaos*. 1996.
42. H.C. DOETS. *Wijzer in Wiskunde*. 1996.
43. Vakantiecursus 1997: *Rekenen op het Toeval*. 1997.
44. Vakantiecursus 1998: *Meetkunde, Oud en Nieuw*. 1998.
45. Vakantiecursus 1999: *Onbewezen Vermoedens*. 1999.
46. P.W. HEMKER, B.W. VAN DE FLIERT (eds.). *Proceedings of the 33rd European Study Group with Industry*. 1999.
47. K.O. DZHAPARIDZE. *Introduction to Option Pricing in a Securities Market*. 2000.
48. Vakantiecursus 2000: *Is wiskunde nog wel mensenwerk?* 2000.
49. Vakantiecursus 2001: *Experimentele wiskunde*. 2001.
50. Vakantiecursus 2002: *Wiskunde en gezondheid*. 2002.
51. G.M. HEK (ed.). *Proceedings of the 42nd European Study Group with Industry*. 2002.
52. Vakantiecursus 2003: *Wiskunde in het dagelijks leven*. 2003.
53. Vakantiecursus 2004: *Structuur in schoonheid*. 2004.
54. Vakantiecursus 2005: *De schijf van vijf – meetkunde, algebra, analyse, discrete wiskunde, stochastiek*. 2005.
55. J. HULSHOF ET AL. (eds.). *Proceedings of the 52nd European Study Group with Industry*. 2006.
56. Vakantiecursus 2006: *Actuele wiskunde*. 2006.
57. Vakantiecursus 2007: *Wiskunde in beweging*. 2007.
58. Vakantiecursus 2008: *Wiskunde en profil – het gezicht van de wiskunde*. 2008.
59. Vakantiecursus 2009: *Tel uit je winst – wiskunde in geld en spelen*. 2009.
60. Vakantiecursus 2010: *Wiskunde: de uitdaging*. 2010.

MC SYLLABI

1.1 F. Göbel, J. van de Lune. Leergang besliskunde, deel I: wiskundige basiskennis. 1965.
1.2 J. Hemelrijk, J. Kriens. Leergang besliskunde, deel 2: kansberekening. 1965.
1.3 J. Hemelrijk, J. Kriens. Leergang besliskunde, deel 3: statistiek. 1966.
1.4 G. de Leve, W. Molenaar. Leergang besliskunde, deel 4: Markovketens en wachttijden. 1966
1.5 J. Kriens, G. de Leve. Leergang besliskunde, deel 5: inleiding tot de mathematische besliskunde. 1966.
1.6a B. Dorhout, J. Kriens. Leergang besliskunde, deel 6a: wiskundige programmering. 1967.
1.6b B. Dorhout, J. Kriens, J.Th. van Lieshout. Leergang besliskunde deel 6b: wiskundige programmering. 1967
1.7a G. de Leve. Leergang besliskunde, deel 7a: dynamische programmering 1. 1969
1.7b G. de Leve, H.C. Tijms. Leergang besliskunde, deel 7b: dynamische programmering 2. 1970.
1.7c G. de Leve, H.C. Tijms. Leergang besliskunde deel 7e: dynamische programmering 3. 1971.
1.8 J. Kriens, F. Göbel, W. Molenaar. Leergang besliskunde, deel 8: minimaxmethode, netwerkplanning, simulatie. 1968.
2.1 G.J.R. Förch, P.J. van der Houwen, RP. van de Riet. Colloquium stabiliteit van differentieschema's deel 1. 1967.
2.2 L. Dekker, T.J. Dekker, P.J. van der Houwen, M.N. Spijker. Colloquium stabiliteit van differentieschema's deel 2. 1968.
3.1 H.A. Lauwerier. Randwaardeproblemen, deel 1. 1967.
3.2 H.A. Lauwerier. Randwaardeproblemen, deel 2. 1968.
3.3 H.A. Lauwerier. Randwaardeproblemen, deel 3. 1968.
4 H.A. Lauwerier. Representaties van groepen. 1968.
5 J.H. van Lint, J.J. Seidel, P.C. Baayen. Colloquium discrete wiskunde. 1968.
6 K.K. Koksma. Cursus ALGOL 60. 1969.
7.1 Colloquium moderne rekenmachines, deel 1. 1969.
7.2 Colloquium moderne rekenmachines, deel 2. 1969.
8 H. Bavinck, J. Grasman. Relaxatietrillingen. 1969.
9.1 T.M.T. Coolen, G.J.R. Förch, E.M. de Jager, H.G.J. Pijls. Colloquium elliptische differentiaalvergelijkingen, deel 1. 1970.
9.2 W.P. van den Brink, T.M.T. Coolen, B. Dijkhuis, P.P.N. de Groen, P.J. van der Houwen, EM. de Jager, N.M. Temme, R.J. de Vogelaere. Colloquium elliptische differentiaalvergelijkingen, deel 2. 1970.
10 I. J. Fabius, W.R. van Zwet. Grondbegrippen van de waarschijnlijkheidsrekening. 1970.
11 H. Bart, M.A. Kaashoek, H.G.J. Pijls, W.J. de Schipper, J. de Vries. Colloquium halfalgebra's en positieve operatoren. 1971.
12 T.J. Dekker. Numerieke algebra. 1971.
13 F.E.J. Kruseman Aretz. Programmeren voor rekenautomaten; de MC ALGOL 60 vertaler voor de EL X8. 1971.
14 H. Bavinck, W. Gautschi, G.M. Willems. Colloquium approximatietheorie. 1971.
15.1 T.J. Dekker, P. W. Hemker, P.J. van der Houwen. Colloquium stijve differentiaalvergelijkingen, deel 1. 1972.
15.2 P.A. Beentjes, K. Dekker, H.C. Hemker, S.P.N. van Kampen, G.M. Willems. Colloquium stijve differentiaalvergelijkingen, deel 2. 1973.
15.3 P.A. Beentjes, K. Dekker, P.W. Hemker, M. van Veldhuizen. Colloquium stijve differentiaalvergelijkingen, deel 3. 1975.
16.1 L. Geurts. Cursus programmeren, deel 1: de elementen van het programmeren. 1973.
16.2 L. Geurts. Cursus programmeren, deel 2: de programmeertaal ALGOL 60. 1973.
17.1 P.S. Stobbe. Lineaire algebra, deel 1. 1973.
17.2 P.S. Stobbe. Lineaire algebra, deel 2. 1973.
17.3 N.M. Temme. Lineaire algebra, deel 3. 1976.
18 F. van der Blij, H. Freudenthal, J.J. de Iongh, J.J. Seidel, A. van Wijngaarden. Een kwart eeuw wiskunde 1946-1971, syllabus van de vakantiecursus 1971. 1973.
19 A. Hordijk, R. Potharst, J.Th. Runnenburg. Optimaal stoppen van Markovketens. 1973.
20 T.M.T. Coolen, P.W. Hemker, P.J. van der Houwen, E Slagt. ALGOL 60 procedures voor begin- en randwaardeproblemen. 1976.
21 J.W. de Bakker (red.). Colloquium programma-correctheid. 1975.
22 R. Helmers, J. Oosterhoff, F.H. Ruymgaart, M.C.A. van Zuylen. Asymptotische methoden in de toe-tsingstheorie; toepassingen van naburigheid. 1976.
23.1 J.W. de Roever (red.). Colloquium onderwerpen uit de biomathematica, deel I. 1976.
23.2 J.W. de Roever (red.). Colloquium onderwerpen uit de biomathematica. deel 2. 1977.
24.1 P.J. van der Houwen. Numerieke integratie van differentiaalvergelijkingen . deel 1: eenstapsmethaden. 1974.
25 Colloquium structuur van programmeertalen. 1976.
26.1 N.M. Temme (ed.). Nonlinear analysis, volume 1. 1976.
26.2 N.M. Temme (ed.). Nonlinear analysis, volume 2. 1976.
27. M. Bakker, P.W. Hemker, P..J. van der Houwen, SJ. Polak, M, van Veldhuizen. Colloquium discretiseringsmethoden. 1976.
28 O. Diekmann, N.M. Temme (eds.). Nonlinear diffusion problems. 1976.
29.1 J.C.P. Bus (red.). Colloquium numerieke programmatuur, deel 1A, deel 1 B. 1976.
29.2 H.J.J. te Riele (red.). Colloquium numerieke programmatuur, deel 2. 1977.
30 J. Heering, P. Klint (red.). Colloquium programmeeromgevingen. 1983.
31 J.H. van Lint (red.). Inleiding in de coderingstheorie. 1976.
32 L. Geurts (red.). Colloquium bedrijfsystemen. 1976.
33 P..J. van der Houwen. Berekening van waerstanden in zeeën en rivieren. 1977.
34 J. Hemelrijk. Oriënterende cursus mathematische statistiek. 1977.
35 P.J.W. ten Hagen (red.). Colloquium, computer graphics. 1978.
36 J.M. Aarts, J. de Vries. Colloquium topologische dynamische systemen. 1977.
37 J.C. van Vliet (red.). Colloquium capita datastructuren. 1978.
38.1 T.H. Koornwinder (ed.). Representations of locally compact groups with applications, part I. 1979.
38.2 T.H. Koornwinder (ed.). Representations of locally compact groups with applications, part II. 1979.
39 O J. Vrieze, G.L. Wanrooy. Colloquium stochastische spelen. 1978.
40 J. van Tiel. Convexe analyse. 1979.
41 H.J.J. te Riele (ed.) Colloquium numerical treatment of integral equations. 1979.
42 J.C. van Vliet (red.). Colloquium capita implementatie van programmeertalen. 1980.
43 A.M. Cohen, H.A. Wilbrink. Eindige groepen (een inleidende cursus). 1980.
44 J.G. Verwer (ed.) . Colloquium numerical solution of partial differential equations. 1980.
45 P. Klint (red.). Colloquium; hogere programmeertalen en computerarchitectuur. 1980.
46.1 P.M.G. Apers (red.). Colloquium databankorganisatie, deel I. 1981.
46.2 P.G.M. Apers (red.). Colloquium databankorganisatie, deel 2. 1981.
47.1 P. W. Hemker (ed.). NUMAL, numerical procedures in ALGOL 60: general information and indices. 1981.
47.2 P.W. Hemker (ed.). NUMAL, numerical procedures procedures in ALGOL 60, vol. 1: elementary procedures; vol. 2: algebraic evaluatons. 1981.
47.3 P.W. Hemker (ed.). NUMAL, numerical procedures in ALGOL 60, vol. 3A: linear algebra part I. 1981.
47.4 P.W. Hemker (ed.). NUMAL, numerical procedures in ALGOL 60, vol 3B: linear algebra, part II. 1981.
47.5 P.W. Hemker (ed.). NUMAL, procedures in ALGOL 60, vol. 4: analytical evaluations; vol. 5A: analytical problems. part I. 1981
47.6 P.W. Hemker (ed.). NUMAL, procedures in ALGOL 60, vol 5B: analytical problems, part II. 1981
47.7 P.W. Hemker (ed.). NUMAL, procedures in ALGOL 60, vol. 6: special functions and constants; vol. 7: interpolation and approximation. 1981
48.1 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). Colloquium complexiteit en algoritmen, deel 1. 1982.
48.2 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). Colloquium complexiteit en algoritmen, deel II. 1982.
49 T.H. Koomwinder (ed.) The structure of real semisimple Lie groups. 1982
50 H. Nijmeijer. Inleiding systeemtheorie. 1982.
51 P.J. Hoogendoorn (red.). Cursus cryptografie. 1983.