Rekenen en getaltheorie

Rede uitgesproken door

Peter Stevenhagen

bij de aanvaarding van het ambt van hoogleraar
in de zuivere wiskunde aan de Universiteit Leiden
op vrijdag 7 september 2001

Postadres van de auteur:

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden

E-mail: psh@math.leidenuniv.nl

Mijnheer de Rector Magnificus, zeer gewaardeerde toehoorders,

Inleiding

De traditie wil dat een zojuist benoemd hoogleraar zijn ambt officieel aanvaardt door in het openbaar uit te leggen wat zijn specialisme zoal behelst. Er zijn niet veel beroepsgroepen die een dergelijke traditie hebben, en U zou hieruit kunnen afleiden dat academici meer moeite hebben dan anderen om de wereld duidelijk te maken wat zij doen, of een sterkere behoefte voelen om hun bestaan in het openbaar te verdedigen. Maar misschien is het gewoon omdat in iedere leraar, een hoogleraar niet uitgezonderd, een schoolmeester steekt, die elke gelegenheid aangrijpt om zijn gehoor te onderrichten. Of dat gehoor dat altijd op prijs stelt is de vraag, maar uit het feit dat U hier in deze harde banken plaats heeft genomen concludeer ik dat U zich niet aan dit vertoon van academische zendingsdrang hebt willen onttrekken, en een verhandeling onder de titel 'Rekenen en getaltheorie' niet uit de weg gaat. Ik zal proberen daar slechts met mate misbruik van te maken.

Het is waar dat niet iedereen door zijn werkgever in staat wordt gesteld om zijn bezigheden toe te lichten in de enigszins plechtstatige ceremonie zoals we die hier vanmiddag kennen; daar staat echter tegenover dat iedereen wel eens geconfronteerd wordt met de informele variant van dit verschijnsel, waarbij hem op een feestje of receptie gevraagd wordt naar zijn studie of beroep. Ook ik heb die vraag in het verleden meer dan eens mogen beantwoorden. en met name in mijn tijd als promovendus was ik wel eens jaloers op mensen die hun dagen vulden met respectabele bezigheden die in een paar woorden aan een willekeurig gesprekspartner medegedeeld konden worden. Als ik meldde dat ik een wiskundige was die onderzoek in de getaltheorie deed leiddde dat zelden tot een begrijpend knikje, en meestal tot een vragend 'getal...theorie?' 'Ja, de theorie van getallen, 1, 2, 3, 4 enzovoorts, net wat je bij getallen denkt', antwoordde ik dan. Want ik bevind mij in de bevoorrechte situatie onder wiskundigen dat iedereen weet wat getallen zijn; voor een topoloog of een logicus ligt dat alweer anders.

De keerzijde van de toegankelijkheid van getallen is dat de reactie vaak luidt: 'getallen, wat kun je daar nou aan onderzoeken?' Of, vaker nog, 'bedoel je dat je berekeningen uitvoert met hele grote getallen?' En voor het geestesoog van mijn gesprekspartner zag ik al het beeld opdoemen van de wetenschapper-in-stofjas zoals die in The Far Side traditioneel geportretteerd wordt: voor een schoolbord vol grote getallen en onbegrijpelijke formules, en meestal voorzien van een uilenbrilletje en een warrige haardos. Ik ben in die tijd lenzen gaan dragen, maar dat hielp niet erg, en ik moest steeds weer uitleggen dat getaltheoretici niet de hele dag op grote schoolborden staartdelingen uitschrijven, of voortdurend getallen die niet meer op een schoolbord passen aan een computer voeren. De meeste wiskundigen houden helemaal niet van formules die eruit zien als een kerstboom, en het opschrijven van getallen van 20 cijfers vinden ze even leuk als een taalkundige het uitspreken van woorden van 20 lettergrepen. Een getaltheoreticus is evenmin een rekenaar als een schrijver een typist is; ze rekenen respectievelijk typen, maar dat is een middel en geen doel op zich. Rekenen is nog geen getaltheorie.

Om uit te leggen wat getaltheorie dan *wel* is probeerde ik, nog steeds op zo'n feestje of receptie, te schetsen wat er allemaal voor leuke *theorie* bestaat voor gewone gehele getallen, en ook voor iets minder gewone gehele getallen. In den regel keek ik dan al snel in een enigszins glazige blik, en werd het raadzaam het thema van het gesprek wat te verleggen.

De laatste jaren heb ik ervaren dat het helemaal niet nodig is om te vertellen wat ik doe, maar dat het volstaat te wijzen op de toepassingen die de getaltheorie in het dagelijks leven zichtbaar maken. In deze tijd van pinpasjes en codenummers voor internettransacties weet namelijk iedereen dat er getallen worden gebruikt voor identificatie en versleuteling, en dat Uw privégegevens te grabbel liggen voor wie de over internet vliegende bits maar kan ontcijferen. Dat ik zelf niet dagelijks met een soldeerboutje pinpasjes in elkaar sleutel of zelfs maar protocollen voor dergelijke pasjes ontwerp blijkt geen bezwaar: mijn bestaan als getaltheoreticus in de moderne maatschappij heeft opeens grote legitimiteit gekregen. Als ik ook nog vertel dat ik colleges geef waarin de theoretische basis van al dit moois aan de orde komt, dan krijg ik in den regel geen glazige maar een bewonderende blik, en blijkt mijn gemiddelde gesprekspartner uiterst tevreden. Je ziet hem denken: mijn belastinggeld wordt goed besteed.

Voor deze oratie heb ik geaarzeld welk aspect ik zou moeten benadrukken. Met de theoretische kant voel ik meer affiniteit, maar die is met name vandaag wat lastig te verkopen. Mijn gehoor bestaat immers voor een groot deel uit twee categorieën van mensen: enerzijds zijn dat mijn vakgenoten, die mij vaak genoeg over getaltheorie hebben horen praten, en aan wie ik helemaal niet uit hoef te leggen wat dat is; en anderzijds zijn dat vrienden, kennissen en familie, van wie ik het zou betreuren als ze me halverwege mijn verhaal met een glazige blik zouden dwingen het onderwerp van mijn oratie alsnog te veranderen. Wat de toegepaste kant betreft: die ligt zoals ik al aangaf minder moeilijk, en een lofzang op de rijke toepassingen van de getaltheorie in coderingstheorie en cryptografie zouden sommigen op prijs stellen, waaronder mijn vader, die zich al 20 jaar afvraagt of ik eigenlijk wel iets *nuttigs* doe. Mijn collega's zouden me echter al snel verwijten de problemen van een wiskundige uit de weg te gaan, en hier een modieus PR-praatje op te dissen. Ik wil daarom proberen elk van beide kanten in bescheiden mate aan de orde te stellen.

Getaltheorie

Laten we beginnen met de getaltheorie, en terugkeren naar de gewone gehele getallen, die zó eenvoudig zijn dat menigeen zich afvraagt wat daar voor theorie voor mag wezen. Getallen zijn uitgevonden om te kwantificeren, te *tellen*, en dat is zo'n basisvaardigheid dat iedereen al vroeg leert om te tellen, tot 10 of tot 100, of hoe ver hij maar wil gaan. Op een gegeven moment realiseer je je dat je in principe elk getal tegenkomt door maar eindeloos door te tellen. Dat is een enigszins academische wijsheid omdat dat ook oneindig lang duurt, en in de praktijk je tong al snel genoeg krijgt van het uitspreken van al die Dagobert-Duck-getallen. Het gaat ook niet om het daadwerkelijke tellen, maar meer om de abstracte gedachte dat er oneindig veel getallen in lineaire ordening achter elkaar staan

om je dat tellen mogelijk te maken.

Niet minder fundamenteel dan het rechtstreekse op-, af- of bijtellen is het concept van *vermenigvuldiging*. Dat is ietsje ingewikkelder, en het is niet voor niets dat men generaties lang tafels van vermenigvuldiging uit het hoofd geleerd heeft, terwijl het begrip opteltafel hoegenaamd onbekend is. Tegenwoordig lijkt het nog slechts een onderscheid tussen twee knoppen op een rekenmachine, maar er is een heus verschil. Additief gesproken, voor de optelling, is er een enkele bouwsteen, de eenheid 1, en ieder getal is uniek te maken door die bouwsteen een aantal keer op zichzelf te stapelen. Multiplicatief gesproken, voor de vermenigvuldiging, kom je niet ver door herhaald met 1 te vermenigvuldigen. Willen we grote getallen uit kleine maken door vermenigvuldiging, dan speelt 1 geen rol van betekenis en treedt een nieuw type bouwsteen op, *priemgetal* genaamd.

Laat ik dat illustreren aan de hand van het stichtingsjaar van de Leidse universiteit, 1575. Dat een mooi rond getal, dat zoals U ziet deelbaar is door 25, oftewel 5 keer 5. In feite is het 25 keer 63, en het getal 63 kent U nog wel uit de tafel van 7, dat is 9 keer 7. Omdat 9 nog als 3 keer 3 te krijgen is zien we dat het getal 1575 multiplicatief opgebouwd is uit twee bouwstenen 3, twee bouwstenen 5, en één bouwsteen 7. De getallen 3, 5 en 7 kunnen niet door vermenigvuldiging uit kleinere getallen gekregen worden en zijn daarmee priemgetallen.

Wat ik U heb laten zien is de *priemfactorontbinding* of *factorisatie* van het getal 1575, en U bent vast niet verbaasd als ik U vertel dat ook ieder ander geheel getal op deze manier uit priemgetallen opgebouwd kan worden. U bent misschien ook niet verbaasd te horen dat 1575 echt alleen maar verkregen kan worden met de goede hoeveelheden drieën, vijven en zevens, en dat je door een priembouwsteen als 2, 11 of 13 te gebruiken nooit het getal 1575 krijgt. Deze *éénduidigheid* van de ontbinding klinkt heel vanzelfsprekend, omdat in de scheikunde een watermolecuul alleen maar uit twee waterstofatomen en één zuurstofatoom verkregen kan worden, en in de kernfysica het aantal protonen en neutronen in een alfadeeltje ook al niet de neiging heeft te variëren. U kunt de priemgetallen wel zien als de 'elementaire deeltjes' waaruit de gehele getallen onder vermenigvuldiging opgebouwd zijn. Maar U moet zo'n analogie ook weer niet al te serieus nemen en denken dat wiskunde een soort afgeleide vorm van natuur- of scheikunde is. Van wat ik U verteld heb over priemfactorisatie kan ik U namelijk een *bewijs* verschaffen, en U hoeft dan ook niet bang te zijn voor een nog niet ontdekte relativiteitstheorie, die U vertelt dat priemfactorontbinding zich voor extreem grote getallen toch net een beetje anders gedraagt. Bovendien spreekt de analogie van elementaire deeltjes U misschien minder aan als U bij Euclides leest dat er oneindig veel verschillende priemgetallen bestaan – en daarvan zijn de hele grote even reëel en stabiel als de kleintjes waarmee we 1575 gemaakt hebben.

Bestaan en éénduidigheid van de priemfactorontbinding van getallen zijn zo fundamenteel in de getaltheorie dat men vroeger wel van de *hoofdstelling van de rekenkunde* sprak. De stelling is eenvoudig en elegant te formuleren, en als U erover nadenkt *niet* een onmiddellijk gevolg van de definitie van een priemgetal, die op zich heel natuurlijk is en niet voor niets al door de Grieken ingevoerd werd. Het is een schoolvoorbeeld van

wat een wiskundige een aantrekkelijke stelling pleegt te vinden: een bondig geformuleerde structuurstelling die je precies vertelt hoe iets in elkaar zit. Zoiets geeft je net als met die elementaire deeltjes in de natuurwetenschappen het gevoel dat je de zaken beter begrijpt, dat je in zo'n multiplicatief oerwoud van grote getallen een eenvoudig ordenend principe gevonden hebt. Niet zo eenvoudig als in het additieve geval, maar toch uiterst transparant.

De hoofdstelling van de rekenkunde, om die wat ouderwetse naam maar weer eens te gebruiken, behoort onmiskenbaar tot de *theorie* van de getallen. Met rekenen in de zin van 'cijferen' heeft hij niets te maken, en als U hem wilt bewijzen is het nuttig noch nodig om daadwerkelijk een expliciet getal als 1575 te ontbinden. U wilt het me hopelijk vergeven dat ik U het *bewijs* van de stelling vanmiddag bespaar. Gegeven het thema van vandaag maakt dit mijn oratie volgens sommigen tot een film zonder liefdesscène—maar ik hoop dat U dat gemis na mijn oratie zult kunnen compenseren. De wijze waarop U dat doet wil ik verder aan Uw eigen fantasie overlaten.

Het bewijs dat ik oversla is een erg leuk bewijs, want het leert je wat de voetangels en klemmen zijn die je moet vermijden als je ooit priemfactorontbinding zou willen ontdekken van andersoortige gehele getallen. Dat is precies de reden waarom wiskundigen opgevoed worden met bewijzen. Het is niet zo dat wiskundigen rare mensen zijn die nooit iets willen geloven voordat ze een bewijs hebben gezien—veel wiskundigen geloven wel degelijk dat bepaalde stellingen waar zijn zonder dat ze er zelf ooit een bewijs van gezien hebben—maar omdat ze graag weten *waarom* iets waar is, en omdat ze zich realiseren dat je niet snel iets interessants kunt bewijzen als je niet eerst de trucs van het vak geleerd hebt aan de hand van bewijzen van anderen. Met de bewijzen die je tijdens je studie ziet vul je je gereedschapskist als wiskundige, en anders dan in de bouw kom je er in de wiskunde bij voortduring achter dat wat je altijd voor een hamer had aangezien onverwacht ook als waterpomptang of slijpschijf dienst kan doen. Het is de verbijsterende effectiviteit van wiskundig gereedschap die het zo leuk maakt om wiskunde te doen. Waarmee ik overigens niet wil zeggen dat het niet leuk zou zijn om bij tijd en wijle echte hamers, waterpomptangen of slijpschijven ter hand te nemen.

Rekenen

Laten we eens kijken wat er gebeurt als we onze hoofdstelling van de rekenkunde in concrete gevallen toe willen passen, omdat we theorie wel mooi vinden maar ook in de praktijk willen kunnen rekenen, en daadwerkelijk getallen ontbinden. Met 1575 waren we snel klaar, want dat is een getal dat alleen maar kleine priemfactoren heeft. In het huidige jargon heten zulke getallen *gladde* getallen. Was na het Leids ontzet onze universiteit ietsje sneller opgericht, zeg in 1574, dan had ik daarnet dat getal voor U moeten ontbinden. Het begin is dan makkelijk, want 1574 is een even getal, namelijk 2 keer 787. Maar vervolgens moet ik 787 factoriseren, en wel op zo'n manier dat U mij gelooft. Met andere woorden, ik moet van allerlei kleine getallen laten zien dat ze 787 *niet* delen, en aan het einde zult U het met me eens zijn dat 787 een priemgetal is – want dat is het. Dat is een enigszins langdurige en onprettige bezigheid, en we mogen ons gelukkig prijzen dat men in Leiden bij de creatie

deze nieuwe universitaire structuur niet nog harder van stapel is gelopen.

In zekere zin is het getal 1574 'karakteristieker' voor wat U kunt verwachten als U zomaar een groot getal neemt en het gaat ontbinden. Er zitten meestal een paar kleine priemfactoren in, en als U die eruit haalt blijft er iets over zonder kleine priemfactoren, en de vraag is: is dit een priemgetal of kan het nog verder worden ontbonden? Als we alle mogelijke delers af willen lopen, dan voelt U wel aan dat dat even duurt, maar u zult zeggen: daar hebben we tegenwoordig toch computers voor, om dat domme werk voor ons te doen?

Het is inderdaad zo dat iedere willekeurige PC tegenwoordig een rekenkracht heeft waar een zaal vol geschoolde rekenaars het tegen aflegt, maar je kunt je afvragen of dat in alle gevallen voldoende is. Het betreft hier in eerste instantie een hele *praktische* vraag; de methode om alle mogelijke delers af te lopen ('trial division') werkt in theorie namelijk altijd—maar de vraag is hoe lang je op het antwoord moet wachten.

Zulke vragen zijn al actueel zolang men computers heeft, en ze worden systematisch bestudeerd in de *complexiteitstheorie*, een gebied dat op de grens van wiskunde en informatica ligt. Hierin gaat men niet na hoeveel minuten een computer van fabrikant X nodig heeft om met rekenpakket Y probleem Z op te lossen, maar bepaalt men intrinsieker de *complexiteit* van een methode om iets uit te rekenen. In plaats van 'methode om iets uit te rekenen' zegt men liever 'algoritme', en er zijn nog een paar nuttige woordjes die ik even wil noemen voor we verder kunnen.

Complexiteit

Wat men van een algoritme wil weten is hoe lang het duurt, of in het ergste geval kan duren, voordat de algoritme het antwoord geeft op invoer van een gegeven lengte. Natuurlijk moet U hier die tijdsduur en die lengte wat formaliseren, maar dat zijn details. Waar het om gaat is hoe de rekentijd groeit als *functie* van de lengte van de invoer.

Laten we bij wijze van voorbeeld eens kijken naar het optellen en vermenigvuldigen van getallen. Ik ga er voor het gemak even van uit dat U ooit op de basisschool geleerd hebt hoe dat gaat. Om op te tellen zet U het tweede getal onder het eerste, en telt de getallen op door steeds twee corresponderende cijfers op te tellen, en als daar 10 of meer uitkomt 1 te 'transporteren' naar het volgende cijferpaar. Voor getallen van 20 cijfers duurt dit twee keer zo lang als voor getallen van 10 cijfers: de rekentijd is dus *lineair* in de lengte van de invoer. Als U met de hand rekent ziet U het voor Uw ogen op papier: lange getallen vormen een lange slang onder optelling: dat is 1-dimensionaal, lineair.

Voor vermenigvuldiging ligt het iets anders. Om een vermenigvuldiging uit te voeren moet U in essentie elk cijfer van het eerste getal vermenigvuldigen met elk cijfer van het tweede getal—daar moest U ooit die tafels voor uit Uw hoofd leren—en vervolgens de zaak geschikt optellen. Als we nu van 10 naar 20 cijfers gaan, gaan we van 100 naar 400 'cijfervermenigvuldigingen', niet twee maar *vier* keer zoveel. Ook het aantal optellingen neemt toe. Op papier ziet U weer direct dat vermenigvuldiging van getallen een patroon geeft dat 2-dimensionaal groeit met de invoer, oftewel *kwadratisch*.

Algoritmen waarvan de rekentijd groeit als een polynoom in de lengte van de invoer—in de gegeven voorbeelden heeft dat polynoom graad 1 respectievelijk 2—heten kortweg *polynomiaal*. Polynomiaal correspondeert in de praktijk ruwweg met 'gemakkelijk te doen'. Anders gezegd: als de invoer van de algoritme op te schrijven is in een acceptabele hoeveelheid tijd, dan kunt U tevens wachten op de uitvoer.

Factoriseren door delers proberen is niet een polynomiale methode. Voor getallen van 10 cijfers moet je delers van ten hoogste 5 cijfers proberen, voor getallen van 20 cijfers delers van ten hoogste 10 cijfers. Per deler is dat weinig werk, maar het *aantal* delingen groeit als de wortel van het getal dat we willen factoriseren – en dat is *exponentieel* in de lengte van het getal. Dit verschil tussen polynomiaal en exponentieel is in de praktijk direct zichtbaar. Iedere computer kan getallen van 100 cijfers in een fractie van een seconde optellen of vermenigvuldigen. Maar het proberen van alle delers van ten hoogste 50 cijfers, of zelfs alle priemdelers van ten hoogste 50 cijfers, is volstrekt ondoenlijk. Het verrichten van 10^{50} opeenvolgende handelingen, hoe eenvoudig ook, duurt namelijk eindeloos. Dat bedoel ik heel letterlijk: als U een miljard delingen per seconde uitvoert met Uw computer—dat is heel veel—bent U nog steeds meer dan 10^{40} seconden bezig. Ook wie als kind al moeiteloos de triljoenen van Dagobert Duck voor zich zag moet nog zijn best doen om zich bij 10^{40} seconden iets voor te stellen. Misschien helpt het als ik U zeg dat de geschatte leeftijd van het heelal om en nabij de 10^{18} seconden bedraagt, zodat de leeftijd van het heelal veel vaker in die 10^{40} seconden past dan de duur van mijn oratie in de leeftijd van het heelal.

In het bijzonder ziet U hieruit dat het wachten op een nieuwe, snellere generatie van microprocessoren of het parallel gebruiken van 100.000 computers geen zoden aan de dijk zal zetten. Een echte verbetering zal uit de wiskunde zelf moeten komen, en dat betekent: niet sneller rekenen, maar efficiëntere methodes gebruiken.

Cryptografie

Voordat ik op efficiëntere methodes om getallen te ontbinden inga wil ik iets zeggen over de rol die de ontbinding van getallen speelt in de cryptografie. U hoort misschien liever: over het *nut* van factorisatie, maar dat is niet wat ik zeg.

We hebben gezien dat het gemakkelijk is om twee priemgetallen van 50 cijfers te vermenigvuldigen tot een getal van zo'n 100 cijfers, maar dat het omgekeerde proces—het ontbinden van dat getal van 100 cijfers—erg moeilijk lijkt voor iemand die die priemgetallen niet kent. Met andere woorden: als U zo'n getal N van 100 cijfers genereert en het publiek maakt, zeg via Uw webpagina, dan zijn de priemfactoren van dat getal in theorie publiek—iedereen kan ze afleiden door N te ontbinden—maar in de praktijk geheim, want U bent de enige die dat de facto kan. Als 'publiek geheim' niet al wat anders zou betekenen zou dit er een aardig voorbeeld van zijn.

Er zijn allerlei aardige stellinkjes over restklassen modulo priemgetallen die tot de 17e en 18e eeuw teruggaan, en die het rekenen modulo een groot getal N heel makkelijk maken zodra U de ontbinding van N kent. Kent U die niet, dan kunt U sommige berekeningen nog steeds doen, maar anderen worden erg moeilijk. Neem bijvoorbeeld een willekeurige

restklasse modulo Uw webpagina-getal N. Dan kan iedereen daar probleemloos de dertiende macht van opschrijven. Maar in omgekeerde richting lijkt niemand behalve U in staat om snel dertiendemachtswortels te trekken modulo N, want de efficiënte methoden die we daarvoor hebben beginnen met het ontbinden van N.

Hiermee heeft U een *cryptografisch protocol* om via internet boodschappen te ontvangen die U alleen zelf kunt lezen, en niet al die hackers die het bericht voorbij zien trekken. U vraagt hiertoe mensen om hun berichten aan U te coderen als één of meer restklassen modulo N—dat is makkelijk, vervang a door 01, b door 02 enzovoort—en vervolgens niet de restklassen zelf, maar hun dertiende macht op te sturen. Dat kan de verzender gemakkelijk doen, en het resultaat is dat U de boodschap wel kunt lezen (want U kunt dertiendemachtswortels trekken), maar verder niemand die N niet kan ontbinden. Dit is, afgezien van wat details, het beroemde RSA-protocol (genoemd naar de ontdekkers Rivest, Shamir en Adleman), dat eind jaren zeventig voorgesteld werd en heel snel populair werd. Het geeft de mogelijkheid veilige boodschappen te versturen zonder dat er ooit geheime sleutels uitgewisseld worden: zowel de versleutelde boodschap (die dertiende macht) als de manier waarop deze gemaakt is zijn publiek, maar het 'ontsleutelen', het decoderen van de boodschap is voorbehouden aan de ontvanger, die de priemfactoren van de modulus N kent.

Wat ik hier heel compact vertel is het begin van een uitgebreid verhaal. Er bestaan vele RSA-achtige protocollen, waarbij niet alleen de boodschap beveiligd is tegen nieuwsgierige buitenstaanders, maar waarbij U bijvoorbeeld ook nog eens zeker weet dat de boodschap daadwerkelijk komt van degene die zegt hem te sturen. Wanneer U de bank bent en meneer A vraagt U via internet een miljoen van zijn rekening aan meneer B over te maken, dan wilt U bijvoorbeeld graag weten dat het bericht echt van meneer A komt—en niet van meneer B die op subtiele wijze de berichten van meneer A aan zijn bank manipuleert. U voelt wel aan dat internet dit soort protocollen tot een zaak van de gewone man gemaakt heeft, en dat verklaart waarom getaltheorie zich tegenwoordig als een zeer toegepaste tak van wiskunde mag beschouwen. Het is namelijk zo dat RSA bepaald niet het enige getaltheoretische protocol is in de cryptografie. Omdat computers zo makkelijk met getallen rekenen, daar zijn ze immers voor gemaakt, kunt U al Uw getaltheorieboeken van de plank trekken om soortgelijke protocollen te ontwerpen. U zoekt dan getaltheoretische procedures met dezelfde aantrekkelijke eigenschappen: één kant op heel snel, zoals vermenigvuldigen, maar in omgekeerde richting erg lastig. En zulke procedures zijn er natuurlijk.

Veiligheid

Voor U nu een systeem als RSA omhelst moet U zich natuurlijk wel eerst afvragen of de veiligheid van zo'n systeem iets is waarop U wilt vertrouwen. Bij de introductie van RSA, in 1976, werd bij wijze van voorbeeld een gecodeerde boodschap modulo een getal van 129 cijfers gegeven, en de verwachting was dat zo'n getal nog vele eeuwen onkraakbaar zou blijven. Nog geen 20 jaar later, in 1994, werd het getal ontbonden—niet door trial division natuurlijk, maar door een methode die de *kwadratische zeef* heet. Inmiddels zijn er alweer

betere methoden dan de kwadratische zeef, en RSA-sleutels van meer dan 150 cijfers zijn al gekraakt. Die getallen van 100 cijfers die ik U net suggereerde moet U dus vooral *niet* gebruiken als U zich tegen serieuze pottenkijkers wilt beschermen. Met 200 cijfers zit U daarentegen op dit moment nog redelijk veilig. U kunt natuurlijk proberen superveilig te werken door moduli van 1000 cijfers te gebruiken, maar dat maakt het protocol direct een stuk logger, en dat kan voor een chipkaartenfabrikant een reden zijn om zo'n protocol niet te gebruiken. Het is een beetje een subtiele balans, en het zal U niet verbazen dat er tegenwoordig een boel vraag is naar mensen die thuis zijn in deze wereld. Ik heb collega's die jammeren dat hun aio's na hun promotie een dik betaalde baan bij een bank nemen in plaats van op een karig postdoc-salaris een onzeker bestaan in het wiskundig onderzoek te ambiëren. Maar dat zijn natuurlijk krokodillentranen.

Is factoriseren moeilijk?

Ik keer nu terug naar de theorie, voor degenen wie al deze frivole toepassingen gestolen kunnen worden, en die blij zouden zijn met een polynomiale factorisatiealgoritme die de hele RSA als sneeuw voor de zon zou laten verdwijnen. Wat voor lol is er voor hen te beleven aan dit soort toepassingen?

Vanuit theoretisch perspectief kun je op twee manieren kijken naar een toepassing die gebaseerd is op de veronderstelde moeilijkheid van een wiskundig probleem. Aan de ene kant kun je proberen te *bewijzen* dat zo'n probleem, bijvoorbeeld factorisatie, intrinsiek moeilijk is. Dat zou een toepassing als RSA een wat meer solide basis geven dan we daar nu voor hebben. Aan de andere kant kun je zo'n toepassing ook te lijf gaan met de hele gereedschapskist van de moderne wiskunde om te laten zien dat het onderliggende probleem helemaal niet zo moeilijk is als men beweert, en daarmee de toepassing om zeep helpen. Over elk van beide benaderingen wil ik iets zeggen.

Laten we eerst eens kijken of er *wiskundige* redenen zijn om aan te nemen dat het factoriseren van een groot getal moeilijk is. Om te beginnen is de formulering van de vraag erg eenvoudig: 'hier is een getal van, zeg, 200 cijfers; wat is zijn priemfactorontbinding?'. Sommige eenvoudig te formuleren vragen zijn moeilijk om de simpele reden dat het antwoord erop zo ingewikkeld is dat er vele duizenden pagina's nodig zijn om het zelfs maar op te schrijven. Dat is hier zeker niet het geval. *Als* iemand met een antwoord komt, dan zal dat uit een stel priemgetallen bestaan die samen niet veel meer dan 200 cijfers hebben, en het is vrij snel te controleren of dat antwoord klopt. Hiermee bedoel ik niet alleen dat we snel na kunnen gaan of de aangeleverde priemgetallen inderdaad als produkt het te ontbinden getal van 200 cijfers hebben, maar ook dat het daadwerkelijk *priemgetallen* zijn, en niet alleen maar getallen waarvan je niet direct een deler vindt.

Dat laatste is wat minder evident, zeker als U die 787 van daarnet nog vers in het geheugen hebt en nog steeds de tijd niet gevonden hebt om na te gaan of ik de zaak niet stiekem opgelicht heb, bijvoorbeeld omdat 787 eigenlijk door 23 deelbaar is.

Als ik in plaats van 787 een getal van 1000 cijfers aan U gepresenteerd had als een priemgetal, dan kunt U toch, misschien niet uit Uw blote hoofd maar wel met een reken-

machine, verifiëren dat dat getal inderdaad priem is. Daarvoor hoeft U niet alle mogelijke delers van ten hoogste 500 cijfers te proberen. U controleert namelijk gewoon of die stellinkjes voor priemgetallen uit de 17e en 18e eeuw die ik zonet al even noemde ook voor Uw getal opgaan. Dat wil zeggen, je pakt een paar restklassen modulo dat getal van 1000 cijfers en controleert met je rekenmachine of ze aan zo'n stellinkje voldoen. Is er een restklasse waarvoor het misgaat, dan is je getal kennelijk niet priem. En komt er steeds uit wat er uit moet komen, voor iedere restklasse die je maar probeert, dan ben je al snel moreel zeker dat je getal inderdaad priem is.

'Moreel zeker' is geen standaard wiskundige terminologie. Stel dat U een ideale munt heeft, laten we zeggen zo'n euromunt die U binnenkort in een kennismakingspakketje krijgt, die bij het opwerpen steeds kop geeft, of U het nu 10 of 20 of 50 keer doet. Dan bent U moreel zeker dat op *beide* zijden van de munt koningin Máxima afgebeeld staat, of wie ook maar een kop voor dit doel beschikbaar heeft gesteld.

Bent U een purist die *wiskundige* zekerheid ambieert, een *bewijs* dus, dan kunt U niet om ingewikkelder wiskunde heen. Omdat wij daar zometeen om efficiënt te factoriseren óók niet omheen kunnen wil ik hier nu verder niet op ingaan. Laat ik slechts zeggen dat het tegenwoordig niet meer als moeilijk geldt om voor een getal van 1000 cijfers dat priem lijkt te zijn een echt bewijs te geven dat het priem is, of om naar believen priemgetallen van 1000 cijfers op te hoesten.

P = NP

Ik keer nu terug naar het factoriseren. We bevinden ons in een situatie dat we een korte, eenvoudig gestelde vraag hebben waarop het correcte antwoord ook weer kort en eenvoudig te formuleren is—maar het lijkt of we dat antwoord van zijn levensdagen niet zullen vinden. Uw eerste gedachte is natuurlijk dat dat een beschamende situatie is, en dat die wiskundigen met al hun slimheid dan maar een betere methode moeten vinden. Het is echter zo dat de wereld met zijn beperkingen komt, en de wiskunde zou de wiskunde niet zijn als het geen theoretisch kader had geschapen voor de vraag of er wiskundige problemen bestaan waarvan de antwoorden wel snel te verifiëren, maar *bewijsbaar* niet snel te vinden zijn. Bij 'snel' moet U natuurlijk denken aan 'polynomiaal', zoals ik U net uitlegde. Deze fundamentele theoretische vraag is het zogenaamde P = NP-probleem, het belangrijkste open probleem uit de complexiteitstheorie. Wie het oplost heeft recht op 1 miljoen dollar van het Clay Institute, en misschien ook wel op de zojuist door de Noorse regering ingestelde Abelprijs, die met ingang van 2002 de rol moet gaan spelen van de niet bestaande Nobelprijs voor wiskunde.

Natuurlijk vormen die miljoenen helemaal geen motivatie om een wiskundig probleem op te lossen. Andrew Wiles heeft niet de laatste stelling van Fermat bewezen omdat er een Wolfskehl-prijs op hem stond te wachten, en niemand gelooft dat de Riemann-hypothese binnenkort bewezen wordt alleen om de simpele reden dat Clay daar ook al een miljoen voor uitlooft.

Ik moet hier overigens aan toevoegen dat het factorisatieprobleem waarschijnlijk niet

een zogenaamd *NP-compleet* probleem is, en dat betekent dat de miljoenen die U met een polynomiaal factorisatiealgoritme kunt verdienen uit een andere hoek zullen komen. U mag zelf verzinnen welke dat is.

Het is in feite zeer wel mogelijk dat factoriseren veel makkelijker is dan al die NP-complete problemen, en dat we alleen maar denken dat het zo moeilijk is omdat we er nog niet in geslaagd zijn om het op een handige manier te doen, en omdat er zoveel mensen zijn die *zeggen* dat het moeilijk is.

Wiskunde om te factoriseren

Zo'n 25 jaar geleden was de heersende gedachte onder experts dat het niet binnen afzienbare tijd tot de mogelijkheden zou behoren om getallen van ruim 100 cijfers te ontbinden. Wie de wiskundige nieuwtjes volgt ziet dat 'recordfactorisaties' al richting 200 cijfers beginnen te kruipen—en anders dan in de topsport, waar je snel tegen de limieten van het menselijk lichaam oploopt, lijken de limieten van de menselijke geest nog niet in zicht. Deze vooruitgang is niet zo zeer het gevolg van de steeds betere computers, als wel van de ontdekking van efficiëntere methodes. Het leuke van die methodes is dat ze gebaseerd zijn op tamelijk actuele wiskunde, van een soort die door weer andere experts wel voor 'theoretische wiskunde' wordt uitgemaakt. Daarmee bedoelen ze: 'niet toepasbaar in de industrie', of 'niet iets waar je snel een patent op krijgt'. Dat blijkt nu wel degelijk het geval. Het is kennelijk erg moeilijk om in de wiskundige toekomst te kijken.

De twee beste methoden van dit moment om een niet-glad getal te ontbinden zijn de *elliptische krommen methode* van Hendrik Lenstra en de *getallenlichamenzeef* van de Engelsman Pollard, die elk hun eigen sterke punten hebben. Zoals de naam aangeeft werken die respectievelijk met elliptische krommen en getallenlichamen, objecten waar je wat minder snel mee in aanraking komt dan met gewone getallen, en die niet op de basisschool, maar pas in doctoraalcolleges wiskunde aan de orde komen. Het zijn geen net ontdekte, splinternieuwe objecten, integendeel. De 18e-eeuwse wiskundige Euler rekende er al lustig op los in getallenlichamen, en manipuleerde met succes elliptische integralen, de toenmalige verschijningsvorm van elliptische krommen. Dat was de pioniersfase, toen men nog nauwelijks wist wat er allemaal voor wonderlijke dingen gebeurden, en in de ruim twee eeuwen die sindsdien verstreken zijn is er een boel veranderd.

De theorie van elliptische krommen heeft sinds zijn oorsprong in de calculus, de analyse zo U wilt, een lange ontwikkeling doorgemaakt, en iedere tijd heeft er zijn steentje aan bijgedragen. Wiskundig gesproken staat die theorie op een kruispunt van diverse stromingen. Het discrete logaritme-probleem op elliptische krommen, dat misschien nog wel moeilijker is dan factorisatie, ligt ten grondslag aan een protocol waarover men op dit moment erg enthousiast is in de cryptografie. Zeker sinds het bewijs van de Laatste Stelling van Fermat in 1995 zijn elliptische krommen een beetje de troeteldieren van de *arithmetische algebraïsche meetkunde*, een zeer actief gebied in de wiskunde, ook in Nederland, waarin meetkunde en getaltheorie met elkaar versmolten zijn. De theorie van de getallenlichamen, meestal *algebraïsche getaltheorie* genoemd, heeft twee eeuwen na Euler

eveneens een natuurlijke plaats binnen de arithmetische algebraïsche meetkunde gevonden.

U moet overigens niet denken dat we na twee eeuwen alles van getallenlichamen en elliptische krommen weten dat er te weten valt. Integendeel, sommige van de meest voor de hand liggende vragen zijn nog wijd open. We hebben nog nauwelijks resultaten voor het 'generieke' gedrag van klassengetallen van getallenlichamen, en wie een fundamentele mededeling voor elliptische krommen als het Birch-Swinnerton-Dyer-vermoeden kan bewijzen krijgt—U raadt het al—een miljoen van het Clay Institute.

Factorisatiemethodes

Pas sinds kort worden elliptische krommen en getallenlichamen gebruikt om te factoriseren, en die mogelijkheid werd als nogal verrassend ervaren, omdat niets in de aard van getallenfactorisatie op een verband met deze objecten wijst. Dit is precies wat ik bedoelde toen ik zei dat in de wiskunde een hamer soms ook een waterpomptang kan zijn. Dat gebeurt de hele tijd in de wiskunde, maar het blijft een bron van verbazing, niet in de laatste plaats voor wiskundigen zelf.

De moderne factorisatiemethodes hebben nog een aardige eigenschap: ze vallen net niet binnen de kaders van de 'klassieke' theorie. In het geval van elliptische krommen wordt die theorie over *lichamen* opgezet, terwijl je om getallen te ontbinden de theorie gebruikt over ringen die geen lichamen zijn. Voor de getallenlichamenzeef ontbind je hulpgetallen over een getallenring die in den regel niet een ring van gehelen is. Dat betekent dat alle tekstboekstellingen, die de U bekende hoofdstelling van de getaltheorie naar de gehele getallen in willekeurige getallenlichamen generaliseren, niet van toepassing zijn. Dat klinkt misschien dramatisch, maar dat is het helemaal niet. Met die problemen kun je namelijk aankloppen bij de arithmetische meetkunde en de commutatieve algebra, specialismen die pas in de twintigste eeuw ontwikkeld zijn, en bepaald niet met het oog op cryptografische toepassingen. Vaak hebben de vaklieden in zo'n hoek de antwoorden klaar, maar soms kom je met vragen waar ze nog nooit over hadden nagedacht, wat misschien nog wel leuker is. Het illustreert fraai hoe arbitrair het soms gemaakte onderscheid tussen zuivere en toegepaste wiskunde kan zijn.

We zien ook dat als je een theorie wilt hebben die in praktische situaties toepasbaar is, bijvoorbeeld op zo'n platvloers probleem als factorisatie, je hem vooral een beetje algemeen op moet zetten. Dat zogenaamde 'abstracte' algemene theorie het beste op de praktijk toegesneden blijkt te zijn behoort geen verrassing te zijn. Het is tenslotte bijna een tautologie dat een algemene theorie ook toepasbaar is op andere problemen dan de directe aanleiding tot het ontstaan van de theorie in kwestie. Het kost wel extra energie om je zo'n algemenere abstracte theorie eigen te maken, en dat maakt het soms aantrekkelijk om te denken dat al die abstractie nergens goed voor is.

De meeste wiskundigen vinden het leuk om te zien hoe sommige 'industriële' vragen steeds meer met 'zuivere' methoden aangepakt worden, en hoe aanvankelijk puur theoretische inzichten onverwachte commerciële toepassingen hebben. Het is wel zo dat de mensen met de fundamentele inzichten vaak niet de commerciële exploitanten zijn, en dat

de meeste wiskundigen hun hart meer aan een van beide kanten hebben liggen. In de algoritmische getaltheorie vind je zowel mensen die schier onpasselijk worden als ze een basis voor een vectorruimte moeten kiezen als mensen die enthousiast worden als ze 10% tijd winnen op hun matrixvermenigvuldiging door bepaalde chips in hun PC van het moment net even slimmer te gebruiken. Dat vult elkaar prachtig aan, en het zou niet best zijn als alle lieden in zo'n vakgebied uit hetzelfde hout gesneden waren.

Onderwijs

Wat ik U meld over de praktische toepasbaarheid van abstractie, de inzetbaarheid van stukken wiskunde in situaties waar je dat niet direct verwacht en de noodzaak van verschillende soorten wiskundigen is niet specifiek iets wat met getaltheorie samenhangt, en zal U ook niet al te verrassend in de oren klinken. Niettemin is het niet iets waar mensen in de praktijk gemakkelijk conclusies aan verbinden. Onvoorspelbaarheid, verrassing en variatie zijn geen grootheden die zich gemakkelijk laten 'managen', zoals dat tegenwoordig heet. Omdat ik deze week mijns ondanks ook een beetje manager geworden ben wil ik daar ter afsluiting iets over zeggen, en wel met betrekking tot het onderwijs.

Wat zou je als student willen van een moderne wiskundeopleiding, eentje die je een beetje beslagen ten ijs laat verschijnen in het onderzoek, in het bedrijfsleven of eventueel in het onderwijs? Je wilt graag zo snel mogelijk, dus nog voordat je je in je favoriete tak van wiskunde specialiseert om daarin af te studeren, dat rijke wiskundige instrumentarium met begrip leren hanteren, en een abstracte vorming hebben die je in staat stelt de structuren te herkennen die ten grondslag liggen aan de problemen waar je op stuit, en weten hoe je je vingers achter zo'n structuur krijgt, met theorie of door op een computer te rekenen. Dat vereist een geschikte combinatie van theorie en praktische vaardigheid.

Voor de theorie is het hoorcollege uitgevonden, waarin iemand uitlegt waarom allerlei ogenschijnlijk ingewikkelde dingen helemaal niet ingewikkeld zijn, maar iets onvermijdelijks hebben en precies gemaakt zijn om te doen wat ze doen. De dingen waarvan iemand je als je nog klein bent uitlegt hoe eenvoudig ze zijn vind je op latere leeftijd inderdaad erg eenvoudig, en je begrijpt niet hoe mensen ze ooit moeilijk hebben kunnen vinden. In de middeleeuwen was je een wijs man als je kon lezen, en bijna een genie als je kon lezen zonder de woorden hardop uit te spreken. Nu geld je als achtergebleven als je dat op je tiende niet kunt. Zo'n tachtig jaar geleden moest je naar Duitsland reizen als je 'abstracte algebra' wilde leren, en kennis maken met ingewikkelde structuren als groepen, ringen en lichamen. Dat gaf je in de wiskunde direct het aanzien gelijk aan dat van een middeleeuwer die kon lezen zonder zijn lippen te bewegen. Nu is er geen wiskundestudent meer die dit alles niet in het begin van zijn studie tegenkomt, en is het haast meer een taalgebruik dan een theorie. Voor een in hoge mate cumulatieve wetenschap als wiskunde, waarin de oude inzichten niet hun waarde verliezen maar een herformulering op grond van nieuwere inzichten krijgen, is dit proces van 'inklinking' van wezenlijk belang. De ideale docent probeert je dan ook op te leiden zoals hij zelf opgeleid had willen worden, zodat je niet zoals hijzelf vroeger tijd verdoet om een elementair inzicht door vallen en opstaan te

verwerven. Hij legt de lat bij voorkeur hoger dan hij zelf als student kon springen.

Voor de praktische vaardigheid werkt men in de wiskunde meestal met *opgaven*, met zorg samengestelde collecties problemen of praktische opdrachten waarop aspirant-wiskundigen hun nieuwe gereedschap kunnen testen, en waarvan de moeilijkheid varieert van bijna triviaal tot zeer pittig. Die opgaven zijn natuurlijk verplicht, en vervangen vaak geheel of gedeeltelijk het tentamen, waarvan je er in de loop van je studie al snel niet veel meer hebt.

Omdat je als modern wiskundige niet alleen moet kunnen schrijven, maar ook moet kunnen praten is het zinnig als je op werkcolleges geregeld opgaven op het bord voor je medestudenten voormaakt, en je je sprekerstalenten verder ontwikkelt door bij tijd en wijle een algemene voordracht te geven in het studentenseminarium of een specialistische voordracht in een gevorderde werkgroep. 'Presenteren en communiceren' heet dat. Oplezen van een blaadje mag nooit—tenzij je een oratie houdt.

Rendement

U vraagt zich misschien af of mijn schets compatibel is met de veelgehoorde uitspraak van opleidingsdirecteuren dat de studie een beetje makkelijk moet zijn, met veel lucht in het programma, omdat anders de door het ministerie voorgeschreven *rendementscijfers* niet gehaald worden. Ze hebben daar zelfs een woord voor uitgevonden: *studeerbaarheid*. Ik moet altijd een beetje lachen om die rendementen, omdat ze bij mijn weten in principe geheel onafhankelijk zijn van de behaalde resultaten. In de Verenigde Staten is hiervoor het begrip 'grading on a curve' geïntroduceerd. In Hollandse termen betekent het dat je voor *iedere* groep van 100 studenten die vak of studie X volgt bij voorbaat besluit dat de beste vijf een tien krijgen, er tien negens worden gegeven, en verder iets als vijftien achten, twintig zevens, vijfentwintig zessen, vijftien vijven, vijf vieren en vijf drieën. Met deze normering is het rendement, het aantal mensen met een voldoende, automatisch 75%. Om een cijfer te geven hoef je de kandidaten alleen maar lineair te ordenen aan de hand van hun examen, huiswerk of wat ook maar. Wat je die 100 mensen probeert te leren, en of dat al dan niet gelukt is, heeft hier helemaal niets mee te maken. En als de minister zijn rendementswensen verandert hoef je alleen maar wat te herschalen—heel gemakkelijk.

Je kunt je zelfs opleidingen met rendementen van bijna 100% voorstellen, waarbij *iedereen* die niet wegloopt na een aantal jaar een diploma uitgereikt krijgt. Een gevolg is natuurlijk wel dat, net als in de Verenigde Staten, het niet zozeer het diploma zelf is waar je wat mee kunt, als wel een bijbehorende verzameling aanbevelingsbrieven van je belangrijkste docenten. Als die cultuur van aanbevelingsbrieven ook in Nederland gemeengoed gaat worden, heb ik er verder geen bezwaar tegen dat de Universiteit Leiden op financiële gronden doctoraaldiploma's gaat verlenen aan mensen die nauwelijks hun naam kunnen schrijven—ze hoeven hun diploma tenslotte alleen maar te ondertekenen. Anders dan vaak gezegd wordt hoeft het gemiddelde niveau van een student daar niet onder te lijden, integendeel: met een gegarandeerd rendement kun je het gemiddelde niveau gemakkelijk optrekken door materiaal van hoge kwaliteit aan te bieden. Dat is niet hetzelfde als

'materiaal voor studenten van hoge kwaliteit'. Bij geschikte presentatie is het namelijk zeer wel mogelijk om zowel de matige student te boeien als de betere student te stimuleren.

Infantilisering

De wiskundeopleiding die ik U net geschetst heb, waar de lat ogenschijnlijk hoger ligt dan de meeste mensen kunnen springen maar de resultaten volgens een standaardkromme geschaald worden, sluit niet naadloos aan bij de Nederlandse gang van zaken. Het aan de orde stellen van onderwerpen die voor sommigen in je groep van leerlingen niet bij voorbaat haalbaar lijken is hier ten lande 'not done'. Om die reden is men twintig jaar geleden al in het basisonderwijs begonnen 'moeilijke' zaken als zinsontleden en cijferen te vervangen door 'onderwerpen voor iedereen' als wereldverkenning of computer-engels, of wat de mode ook maar voorschrijft. Op dit moment wordt op de middelbare school de eerste drie jaar een soort basisschool gedaan onder de noemer 'basisvorming', zodat niemand 'aansluitproblemen' ondervindt en je voor je vijftiende niet achter kunt raken met wat dan ook. U raadt het al: op de universiteiten wordt tegenwoordig ook over een aansluitingsproblematiek gepraat; de universiteiten zouden op hun beurt rekening moeten houden met een generatie jongeren die door het *studiehuis* zodanig getekend is dat een hoorcollege van meer dan 30 minuten te zwaar is voor hun prille hersenen. Voor de wiskunde hebben we nog het aanvullend probleem dat in de schoolwiskunde een zogenaamd 'realisme' de boventoon voert, waarin rechthoeken tuintjes heten en de stelling van Pythagoras iets is om je hond mee uit te laten. Het is waar dat honden en tuintjes beter aansluiten bij de belevingswereld van iedere kleuter, en dat de mens steeds langer leeft, maar je kunt je afvragen of je ernaar wil streven de intellectuele volwassenwording van een generatie tot na het dertigste levensjaar uit te stellen, uit angst dat er anders af en toe iemand is die iets niet begrijpt. Veel dingen leer je vanaf het moment dat je er aan blootgesteld wordt—en zeker in de wiskunde kan dit beter eerder dan later gebeuren. Ik geloof niet zo in die horden van kinderen die de draad maar kwijt zouden raken. Zonder intellectuele uitdaging raak je ook nog eens hun belangstelling kwijt, en dat is veel erger.

U vraagt zich wellicht af of het inderdaad zo'n vaart loopt met wat ik maar gekscherend de infantilisering van het onderwijs zal noemen. Het onderwijs in Nederland wordt namelijk op alle niveaus voortdurend hervormd, en de meeste van die hervormingen beschrijven in de tijd een slingerbeweging tussen veel of weinig vakken, concretie en abstractie, modern en klassiek, of wat U maar wilt. Persoonlijk lig ik er absoluut niet wakker van dat een wiskundeboek op de middelbare school tegenwoordig aan elkaar hangt van kleurige kadertjes die door foto's omlijst worden, en het geheel nog eens verluchtigd wordt met heel erg grappige stripjes—ook kinderen weten het kaf vaak wel van het koren te scheiden. Ook niet zo erg is het als kinderen wordt geleerd om vergelijkingen op te lossen door als stap 1 het linkerlid groen en het rechterlid rood te kleuren—zoiets onzinnigs leer je tenslotte ook heel gemakkelijk weer af. Jammer is het wel dat wiskunde op school zo soms verwordt tot het afdraaien van een standaardalgoritme door gedresseerde aapjes—dat maakt het niet makkelijk om het vak leuk te vinden. Wellicht is dit de prijs die de universitaire wiskunde

betaalt voor het jarenlang negeren van de schoolwiskunde—daar worden nu de curricula en de lesmethoden in hoofdzaak door anderen bepaald.

Leraren

Meer nog dan andere vakken, die naar hun aard dichter bij het dagelijks leven staan, staat of valt een wat abstracter vak als wiskunde met de persoon van de leraar, die door zijn voorbeeldrol het vak voor de gemiddelde leerling personifieert. Is de leraar niet geïnspireerd, dan is het vak niet inspirerend. Weet de leraar niet hoe echte wiskunde werkt, dan komt de leerling er ook niet achter. Het treft nu ongelukkig dat steeds meer leraren op middelbare scholen nog nooit een universiteit van binnen hebben gezien, en dat omgekeerd onder de studenten wiskunde weinig animo voor het leraarschap bestaat.

Het is relatief recent dat universiteiten zich hier zorgen om maken, met name in de exacte hoek, en dat is niet op grond van een nobel verantwoordelijkheidsgevoel jegens de maatschappij, maar omdat de dalende studentenaantallen onprettige financiële consequenties beginnen te krijgen. Deze faculteit ondervindt dit financiële probleem aan den lijve, en de voorgestelde bezuinigingen hebben zelfs het meinummer van een blad als Science gehaald. Op dezelfde pagina waar Leiden figureert lezen we overigens dat Stanford een half miljard euro gekregen heeft van Hewlett-Packard (of correcter: de Hewlett Foundation). U hoort het goed: een half *miljard*. En de euro is geen lire. Of correcter: slechts voor een deel de lire. De Leidse tekorten bedragen maar een fractie van wat Stanford op dat half miljard aan *rente* krijgt—of U dat geruststellend vindt mag U zelf weten.

Het is overigens niet terecht om de scholen de 'schuld' te geven van die tanende β-belangstelling, die helemaal niet typisch Nederlands is. Het lijkt me wel duidelijk dat de universiteiten hun verantwoordelijkheid voor het opleiden van leraren serieuzer moeten nemen. Daarmee bedoel ik in de eerste plaats dat er een einde moet komen aan de rare situatie dat wiskunde tot op hoog niveau onderwezen wordt door mensen die nog nooit een echte wiskundige van dichtbij hebben gezien. Ik zeg niet dat alle leraren academisch geschoold dienen te zijn, of dat niet-academisch geschoolde leraren niet goed les zouden geven. Maar de steeds wijder wordende kloof tussen school en universiteit die nu ontstaat is nadelig voor beide partijen, en heeft naar ik hoop inmiddels zijn langste tijd gehad. In de tweede plaats schijnt het mij toe dat een universitaire opleiding tot wiskundeleraar stevig ingebed moet zijn in een wiskundestudie, en niet, zoals ik wel meegemaakt heb, een losse flodder waarvoor je langdurig naar een centraal didactisch instituut gestuurd wordt om aan praatgroepen over leerprocessen deel te nemen.

Ik realiseer mij dat dit geen veranderingen zijn die je van de ene op de andere dag invoert, al was het maar omdat je daarmee bestaande machtsposities aantast. Maar als er überhaupt een voordeel is aan een toestand van permanente hervorming en reorganisatie, dan is het wel dat je scheefgegroeide situaties makkelijker aan kunt pakken. Er lijkt me geen reden dat dat niet in goed overleg tussen alle belanghebbenden zou kunnen geschieden. Op de universiteit kunnen we wellicht de introductie van het bachelor-master-systeem ook hiervoor als aanleiding gebruiken.

Profilering

Op korte termijn proberen de universiteiten wel studenten te trekken door een zogenaamde 'profilering'; er gaan wel eens stemmen op die zeggen dat 'Mathematisch Instituut' veel te duf klinkt, en dat je je beter 'Research Institute for Cryptography en Computational Science' kunt noemen. Dat Engels is niet alleen om het prestigieus te laten klinken, en om aan te geven dat wij het Stanford van de geestgronden zijn, maar ook om te laten blijken dat wij bij gebrek aan Nederlandse interesse niet zullen aarzelen de collegebanken te vullen met Oosteuropeanen en Noordafrikanen. Het noemen van gebieden die op dit moment in de belangstelling staan zal niet alleen scholieren trekken, die van wiskunde alleen maar weten dat het duf klinkt, maar het tevens makkelijker maken om fondsen te verwerven. Onze nationale organisatie voor wetenschappelijk onderzoek NWO, die alweer tien jaar geleden het woord 'zuiver' uit haar naam schrapte, wil namelijk graag wiskunde subsidiëren op 'raakvlakken'. Ik twijfel er zelf ten zeerste aan of scholieren die geen wiskunde willen studeren wel cryptografie gaan doen, en of de wiskunde zich thematisch laat sturen door geldschieters.

Ik noemde al een paar keer die prijsjes van meneer Clay, en tot zijn rechtvaardiging moet ik daar aan toevoegen dat zijn instituut niet alleen heel veel geld belooft aan wie die prestigieuze problemen oplost. Wiskunde is namelijk geen loterij, en het is waarschijnlijker dat U de Staatsloterij wint dan dat U morgen bij de koffie per ongeluk een efficiënte factorisatiealgoritme ontdekt. Wiskunde bloeit op instituten en in landen met een goede wiskundige cultuur, waar slimme jongens en meisjes de kunst afkijken van de voorgaande generatie, en uiteindelijk verder kijken door op de schouders van hun leermeesters te gaan staan. De romantische gedachte dat geïsoleerde briljante jongelingen na het lezen van een populariserend boek wel even de wereld om de oren slaan met de oplossing van zo'n Clay-probleem is niet realistisch, en meneer Clay gebruikt zijn geld dan ook in de praktijk om alle soorten van wiskundecongressen te subsidiëren en om jongeren in staat te stellen op goede instituten te verblijven. Wil je zo'n instituut zijn, dan moet je zorgen dat je de best mogelijke mensen in dienst hebt als leermeesters, en je niet te veel bekommeren om wat hun specialisatie is. Die mensen gaan namelijk langer mee dan de modes van het moment.

Stelt U zich maar eens voor dat theoretische fysica toepassingen heeft, en dat over 10 jaar de eerste quantumcomputers in de laboratoria staan. Dan kan mijn oratie direct de prullenbak in, want zulke computers kunnen in polynomiale tijd factoriseren. U kunt wel raden dat zowel wis- en natuurkundigen als informatici zich enthousiast op dit gebied zullen storten, en als de quantum-ICT de beurskoerzen opstuwt komen de studenten misschien ook wel. Dan kun je toch niet de universiteit zijn die in hoofdzaak gericht is op de biomoleculaire wonderen waar men aan het begin van de eeuw zo hoog van opgaf?

Dankwoord

Een oratie is niet compleet zonder een dankwoord, en ook ik wil ten slotte mijn dank uitspreken, om te beginnen aan het College van Bestuur van de Universiteit, voor het vertrouwen dat het met deze benoeming in mij uitspreekt.

Hooggeleerde Lenstra, beste Hendrik, het is niet meer dan passend dat ik me eerst tot jou richt. Mijn komst naar Leiden hangt immers nauw samen met jouw terugkeer naar Nederland, en de creatie van het zogenaamde 'speerpunt getaltheorie' dat we nu in Leiden hebben. Toen ik wegging uit Amsterdam, waar ik een eigen getaltheoriewinkeltje had, had ik collega's die mij vroegen of het niet moeilijk zou zijn om zo dicht naast mij een coryfee en Spinoza-laureaat te hebben. Bovendien kennen ze jou nog wel in Amsterdam, en weten ze dat je over nogal wat zaken sterke meningen hebt, en niet aarzelt die met veel stelligheid naar voren te brengen, al dan niet vergezeld van de mededeling dat je inmiddels de leeftijd bereikt heb waarop je je vooroordelen oordelen mag noemen. Ik weet niet of mijn collega's serieus dachten dat ik, om een andere favoriete uitdrukking van je te gebruiken, hier in Leiden stilletjes langs de plint zou gaan kruipen—maar ik denk eigenlijk van niet. Beste Hendrik, wij kennen elkaar al zo lang en zo goed, en hebben al zo'n gevarieerde record van samenwerking, dat het ondenkbaar is dat er niet nog vele jaren van prettige samenwerking te komen staan. Ik zie het als een groot voorrecht om onder deze omstandigheden te kunnen werken.

Hooggeleerde van Dijk, beste Gerrit, jij hebt me met ingang van deze week opgenomen in het zogeheten Management Team van ons instituut. Als het waar is dat de Engelse taal prestige verleent, dan zal de zaal vast erg onder de indruk zijn van mijn toetreden tot dit uiterst selecte gezelschap. Je hebt waarschijnlijk al gemerkt dat ik als niet altijd even diplomatieke Amsterdammer nog wel enige inwijding in de Leidse bestuurskunst kan gebruiken, en ik wil je bij voorbaat danken voor de steun die ik hierbij van jou als ervaren bestuurder hoop te genieten.

Jean-Claude et Maryfrance, vous êtes parmi les quelques personnes dans cette salle auxquelles je dois présenter mes excuses. Malgré son sujet assez terrestre, mon discours a dû vous rester quelque peu obscur pour des raisons linguistiques. Encore ce matin, une mathématicienne m'a demandé si je voulais bien prononcer mon discours en français. Elle était française, donc ce n'était peut-être pas une blague. Il y a parfois des problèmes pour lesquels je ne trouve pas de solution. Merci pourtant d'être venus, et d'avoir écouté avec patience. La fin est proche.

Lieve Armelle, je hebt me gezegd dat je het absoluut overbodig vond om jou hier te bedanken, maar een film zonder liefdesscène kun je niet ook nog eens afsluiten zonder je vrouw te bedanken. Vroeger was dat heel makkelijk, je kon gewoon zeggen dat je het nooit zo ver geschopt had zonder de voortdurende steun van je vrouw, die het huishouden gaande hield en de kinderen opving terwijl je rustig zat te werken. Nu hoor ik bij de generatie van hoogleraren die zich bijna dagelijks naar huis spoedt om de sluitingstijd van een crèche te halen, en je wilt in zo'n dankwoord de waarheid nu ook weer niet al te zeer geweld aandoen. Dus tegenwoordig kun je je vrouw bedanken omdat ze je er bij tijd en wijle aan

herinnert dat er nog leven buiten je werk is. Misschien moet ik nog een stapje verder gaan en jóu erop wijzen dat jij ook een leven naast je werk hebt, en dat je binnen een gezin een bepaald evenwicht moet vinden. Dat blijft natuurlijk zoeken, maar ik verwacht toch dat we daar de komende jaren steeds beter in zullen slagen. Ik verheug me nu al op jouw inbreng!

Dit publiek vertoon van dankbaarheid brengt mij aan het einde van mijn verhaal. Mocht U nog vragen hebben over die getaltheorie, dan trekt U mij gewoon even aan mijn mouw, op een feestje of receptie.

Ik heb gezegd.