Vakantiecursus 2010

Voor leraren in de exacte vakken aan havo, vwo, hbo leerlingen en andere belangstellenden organiseert het Centrum Wiskunde & Informatica (CWI) in 2010 een vakantiecursus met als thema:

Wiskunde: de uitdaging

Ook dit jaar betreft het een tweedaagse cursus, die zowel in Amsterdam als in Eindhoven wordt gehouden en wel op **vrijdag 27 augustus** en **zaterdag 28 augustus** bij het CWI, Science Park 123 (voorheen Kruislaan 413) te Amsterdam, en op **vrijdag 3 september** en **zaterdag 4 september** in het Auditorium van de Technische Universiteit Eindhoven, Den Dolech te Eindhoven. (zie pagina 19 voor de routebeschrijving)

De cursus is voor wiskundedocenten van elk niveau toegankelijk. De deelnemers ontvangen bij aanvang van de cursus een syllabus met teksten van de voordrachten. Het cursusgeld bedraagt €75. Voor studenten van lerarenopleidingen is het cursusgeld slechts €25.

Bij de cursus is inbegrepen een warme maaltijd op vrijdag en een lunch op zaterdag.

Aanmelding

Aanmelding voor deelname aan de cursus kan:

- door het aanmeldingsformulier achter in deze brochure in te vullen en vóór 17 augustus 2010 op te sturen aan het CWI;
- via de website http://www.cwi.nl/nl/vc2010 waar een online registratieformulier ingevuld en opgestuurd kan worden, eveneens vóór 17 augustus 2010.

Deze cursus geldt als nascholingsactiviteit. Voor geïnteresseerden is een nascholingscertificaat beschikbaar. Degene die daar prijs op stelt, gelieve het betreffende formulier in te vullen of dit via het elektronische registratieformulier aan te geven.

Deze cursus wordt mede mogelijk gemaakt door een subsidie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO).

Programma Amsterdam

27 augustus en 28 augustus 2010

vrijdag 27 augustus

Wijzigingen voorbehouden.

15.00-15.25	Ontvangst, koffie
15.25-15.35	Intro 'Wiskunde: de uitdaging' Prof.dr. J.J.O.O. Wiegerinck
15.35-16.20	Verrassende wiskunde bij de olympiade Dr. Quintijn Puite
16.20-16.45	Pauze
16.45-17:30	Boeven vangen met een Bayes net Prof.dr. Marjan Sjerps
17.30-18.30	Diner
18.30-19.15	Gênante problemen Dr.ir. Ionica Smeets
19.15-19.45	Pauze
19.45-20.30	Chaos, voorspelbaarheid, en bemonstering Prof.dr.ir. Jason Frank

zaterdag 28 augustus

10.00-10.30	Ontvangst, koffie
10.30-11.15	Een onmogelijke uitdaging: Diophantische vergelijkingen Prof.dr. Frits Beukers
11.15-12.00	De uitdagende vraagstukken van bedrijven Dr. Vivi Rottschäfer
12.00-13.00	Lunch
13.00-13.45	Hoe je het cryptosysteem RSA soms kunt kraken Dr. Benne de Weger
13.45-14.15	Pauze
14.15-15.00	Rijen Prof.dr. Arnoud van Rooij
15.00-15.05	Sluiting

Programma Eindhoven

3 september en 4 september 2010

vrijdag 3 september

Wijzigingen voorbehouden.

15.00-15.25	Ontvangst, koffie
15.25-15.35	Intro 'Wiskunde: de uitdaging' Prof.dr. J.J.O.O. Wiegerinck
15.35-16.20	Verrassende wiskunde bij de olympiade Dr. Quintijn Puite
16.20-16.45	Pauze
16.45-17:30	Boeven vangen met een Bayes net Prof.dr. Marjan Sjerps
17.30-18.30	Diner
18.30-19.15	Gênante problemen Dr.ir. Ionica Smeets
19.15-19.45	Pauze
19.45-20.30	Chaos, voorspelbaarheid, en bemonstering Prof.dr.ir. Jason Frank

zaterdag 4 september

10.00-10.30	Ontvangst, koffie
10.30-11.15	Een onmogelijke uitdaging: Diophantische vergelijkingen Prof.dr. Frits Beukers
11.15-12.00	De uitdagende vraagstukken van bedrijven Dr. Vivi Rottschäfer
12.00-13.00	Lunch
13.00-13.45	Hoe je het cryptosysteem RSA soms kunt kraken Dr. Benne de Weger
13.45-14.15	Pauze
14.15-15.00	Rijen Prof.dr. Arnoud van Rooij
15.00-15.05	Sluiting

Ten geleide

Prof.dr. Jan Wiegerinck

Korteweg-de Vries Instituut voor Wiskunde (UvA)
e-mail: J.J.O.O.Wiegerinck@uva.nl

De vakantiecursus wordt georganiseerd door het CWI (Centrum Wiskunde & Informatica), in samenwerking met de NVvW (de Nederlandse Vereniging van Wiskundeleraren) onder auspicieën van NWO (de Nederlandse Organisatie voor Wetenschappelijk Onderzoek). Dit jaar wordt de cursus voor de 64e keer georganiseerd.

Het thema is 'wiskunde: de uitdaging'. Daar kun je alle kanten mee op, maar de uitdaging heeft dit jaar in het bijzonder te maken met de uitdaging die de Internationale Wiskunde Olympiade biedt. Deze zal immers in 2011 in Nederland worden gehouden. De voordracht van **Quintijn Puite** sluit direct bij dit thema aan.

Ionica Smeets snijdt lichtvoetig een teer onderwerp aan met Gênante Vragen. Wiskundige vragen die iedere gek kan stellen, maar geen 1000 wijzen kunnen beantwoorden. Wel een wiskundige uitdaging natuurlijk!
Maar zo gauw je over uitdagingen gaat praten blijkt al snel dat er vele uitdagingen voor de wiskunde bestaan en in de wiskunde aanwezig zijn.

Vivi Rothschäfer 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 dat precies in elkaar zit zal **Marjan Sjerps** ons uitleggen.

Het voorspellen van het weer, hoe moeilijk dat is 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. Meer zuiver wiskundig, maar niet minder uitdagend zijn de zaken waar **Frits Beukers** en **Arnoud van Rooij** over spreken. Diophantische vergelijkingen (vergelijkingen waarvan de 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!

Verrassende wiskunde bij de olympiade

Dr. Quintijn Puite

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

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 krijgen de leerlingen veel nieuwe theorie, van modulorekenen en de kleine stelling van Fermat tot de concurrentiestelling van Ceva. Maar behalve deze `hogere wiskunde', komen ook elementaire bewijsprincipes ruimschoots aan bod.
Een voorbeeld is het ladenprincipe: als je $n+1$ balletjes in n laatjes stopt, dan is er ten minste één laatje dat meer dan één balletje bevat. Ook al is dit principe zelf nogal eenvoudig, je kunt het soms op een zeer verrassende manier inzetten om de meest ingewikkelde opgaven op te lossen. In de lezing staat een aantal van zulke 'gezond-verstand-technieken' centraal.
Om u een voorproefje te geven, nodig ik u uit om zich alvast in de volgende drie problemen te verdiepen. We zullen tijdens de lezing van elk van deze opgaven een even simpele als geniale oplossing bekijken.

1. 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?

2. 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.

3. 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).

Boeven vangen met een Bayes net

Prof.dr. Marjan Sjerps

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

Forensische statistiek

Forensische statistiek is een nieuwe en sterk groeiende tak van statistiek en kansrekening, toegepast op het strafrecht. Het onderzoek concentreert zich op de interpretatie van (forensisch) bewijsmateriaal. Kernvragen zijn daarbij: '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 forensische statistiek maakt gebruik van een kansmodel om bovenstaande vragen in concrete strafzaken te beantwoorden. De ingrediënten van dit model zijn hypothesen H_p en H_d van de aanklager resp. de verdediging (van *prosecution* resp *defence*), bewijsmateriaal E (van *evidence*), en de context van de zaak en achtergrondinformatie I (van *information*). Hieruit kan het aannemelijkheidsquotiënt (*Likelihood Ratio*, *LR*) worden berekend:

$$LR = \frac{\mathrm{P}[\mathrm{E} \mid \mathrm{H_p}]}{\mathrm{P}[\mathrm{E} \mid \mathrm{H_d}]}$$

I wordt hierbij in teller en noemer bekend verondersteld. De teller van de *LR* geeft weer hoe goed het bewijsmateriaal past bij de hypothese van de aanklager, en de noemer geeft weer hoe goed het past bij de hypothese van de verdediging. Naarmate het bewijs beter past bij de hypothese van de aanklager en slechter bij die van de verdediging, 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. 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.

Bayesiaanse netwerken

De *LR* kan in forensisch DNA onderzoek vaak daadwerkelijk worden uitgerekend. Voor de vraag hoe een DNA-spoor kan zijn overgedragen van bijvoorbeeld een verdachte op een slachtoffer worden de formules echter al snel te moeilijk. Dit geldt ook voor overdracht van andere typen forensisch bewijs, zoals glasfragmenten, textielvezels, of schotresten, en voor het bepalen van de bewijskracht van de combinatie van verschillende bewijsmiddelen. Er is een nieuwe techniek uit de kansrekening, Bayesiaanse netwerken, die hier een oplossing biedt. Deze grafische modellen hebben de potentie om uit te groeien tot de SPSS van de kansrekening (voor wie dit niets zegt: SPSS is één van de grootste software pakketten voor statistische analyses).
Met een Bayesiaans netwerk kan de *LR* ook worden berekend in complexe situaties op basis van kansinschattingen van één of meer deskundigen. Een Bayesiaans netwerk maakt hierbij bovendien de redenatie inzichtelijk: welke factoren worden beschouwd, hoe zwaar wegen zij, hoe hangen zij samen, en op welk punt verschillen de deskundigen van mening? Het gaat hierbij meer om de ordegrootte van de getallen dan om het laatste cijfer achter de komma. Wanneer er echter te veel onzekere factoren zijn kan er geen waarde worden gehecht aan de getallen en is het model alleen nuttig om de gedachten te structureren.
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. Voor wiskunde docenten zijn forensische statistiek en Bayesiaanse netten interessant om stof uit de kansrekening en statistiek op aansprekende wijze te illustreren. Leerlingen kunnen daarbij eenvoudig zelf Bayesiaanse netten maken met behulp van gratis via internet beschikbare software (Genie).

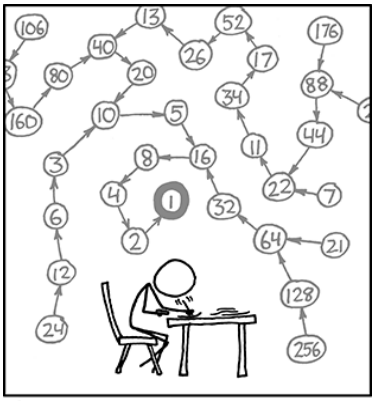
Gênante problemen

Dr.ir. Ionica Smeets

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

Natuurlijk weet u dat er open vraagstukken zijn in de wiskunde. Daarbij denkt u waarschijnlijk aan grote, moeilijke problemen als de Riemann-hypothese. Maar er zijn ook allerlei gênante open problemen. Problemen die eenvoudig te formuleren zijn. Problemen waarvan je zou denken dat ze al eeuwen geleden opgelost zijn, maar waar niemand nog een bewijs voor heeft gevonden.

Zitten er bijvoorbeeld oneindig veel enen in de decimalen van π?



THE COLLATZ CONJECTURE STATES THAT IF YOU PICK A NUMBER, AND IF IT'S EVEN DIVIDE IT BY TWO AND IF IT'S ODD MULTIPLY IT BY THREE AND ADD ONE, AND YOU REPEAT THIS PROCEDURE LONG ENOUGH, EVENTUALLY YOUR FRIENDS WILL STOP CALLING TO SEE IF YOU WANT TO HANG OUT.

Niemand die het weet. Of neem het gekmakende vermoeden van Collatz.
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. Deze stappen blijf je herhalen. Het vermoeden van Collatz is dat je uiteindelijk altijd uitkomt op één, met welk getal je ook begint.
Probeer het maar eens met 6 of 27 als begingetal. Het lijkt altijd te werken, maar een bewijs voor dit vermoeden is er niet. Zo zijn er nog veel meer gênante wiskundige problemen.
Ionica Smeets (wiskundemeisjes.nl) schaamt zich gelukkig nergens voor en bespreekt vandaag een aantal van deze prachtige problemen met u. Ze zal ook vertellen wat wiskundigen wél kunnen.

Chaos, voorspelbaarheid, en bemonstering

Prof.dr.ir. Jason Frank

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

In de jaren 60 van de vorige eeuw wist de Amerikaanse wiskundige en meteoroloog E.N. Lorenz met gebruik van computersimulaties aan te tonen wat al eeuwen intuïtief erkend was in de spreuken van boeren en zeevaarders —het weer is moeilijk voorspelbaar.

> *Al doet april ons mooi weer aanschouwen, 't is even als fortuin, we kunnen hem niet vertrouwen.*
>
> *Is de eerste juli regenachtig, gans de maand is twijfelachtig.*

In veel toepassingen worden wiskundige modellen, in de vorm van differentiaalvergelijkingen, bestudeerd met gebruik van numerieke simulaties. Sinds het werk van Lorenz is bekend dat zulke stelsels niet-lineaire differentiaalvergelijkingen zich zeer complex kunnen gedragen en deterministische chaos kunnen tonen, waardoor de oplossing zeer gevoelig is voor kleine storingen. Zulke chaotische systemen worden routinematig opgelost in onder andere de meteorologie, ongeacht het feit dat door hun chaotische aard de fouten in de benaderde oplossingen exponentieel groeien, en al gauw de hele berekening overheersen. De groeitijd is echter afhankelijk van de begintoestand, zoals wordt verbeeld in Figuur 1, die de evolutie laat zien van een hele verzameling van oplossingen (een zo-geheten ‘ensemble simulatie’) van de befaamde Lorenz attractor. Wat betreft weersvoorspelling, komt dit voorbeeld overeen met het intuïtieve idee dat stabiel weer langer te voorspellen is dan onstabiel weer.
Op langere tijdsintervallen, zoals die van interesse in klimaatstudies en moleculaire dynamica, is er echter geen hoop om een individueel traject nauwkeurig te voorspellen. Liever, het doel van lange simulaties is het bemonsteren van een onderliggende kansdistributie die het statistische evenwicht van het model beschrijft. Men zou hiermee (misschien) de volgende spreuken kunnen kwantificeren:

> *Februari is nooit zo fel, of ze geeft drie lentedagen wel*. (Wat is de waarschijnlijkheid van drie ‘lentedagen’ in februari.)
>
> *Zelfs een kapotte barometer, weet het ooit een keertje beter* (Een barometer geeft een vaste druk X aan, wat is de waarschijnlijkheid dat de werkelijke druk hoger is dan X.)

Figuur 1. Ensemble simulaties van het systeem Lorenz (1963) met verschillende graden van voorspelbaarheid. (Bron: Tim Palmer, ECMWF.)

Het direct berekenen van een waarschijnlijkheid is vaak niet praktisch, omdat het gaat om een integraal in zeer hoge dimensies. In plaats daarvan gebruikt men een lange numerieke simulatie (of een ensemble van meerdere) om de waarschijnlijkheid te benaderen.
Bemonsteren in deze zin stelt twee eisen aan de methode: ten eerste moet de evenwichtsdistributie van de numerieke methode overeenkomen met die van het continue model, ten tweede moet de discrete reeks voldoende chaotisch zijn om de hele ruimte te verkennen. Het eerste ingrediënt eist speciale methoden. De tweede is moeilijk vast te leggen, maar geldt vaak in de praktijk in een voldoende benaderende zin.
In dit college bespreken we de samenhang tussen dynamische systemen, chaos theorie, numerieke methoden, en statistiek.

Een onmogelijke uitdaging: Diophantische vergelijkingen

Prof.dr. Frits Beukers

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

We weten dat $x^2+y^2=1$ de vergelijking is van een cirkel en $x^2-161y^2=1$ de vergelijking van een hyperbool. De bijbehorende meetkundige plaatjes zijn ons allemaal welbekend en strict genomen bestaan deze uit de punten met reële x,y –coördinaten op deze figuren. Wij zullen ons beperken tot de vraag of er ook punten op deze krommen liggen waarvan de x,y -coördinaten geheel of zelfs rationaal zijn. Op deze manier komen we tot de diophantische vergelijkingen, dat wil zeggen vergelijkingen in één of meer onbekenden waarvan we bovendien verlangen dat ze rationaal of geheel zijn. Eén van de beroemdste vergelijkingen is natuurlijk Fermat's $x^n+y^n=z^n$ in de gehele getallen x,y,z.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS

De naam `diophantische vergelijking' stamt van Diophantus van Alexandrië, de Griekse wiskundige uit ongeveer 200 A.D die de Arithmetica schreef, waarvan hier het voorblad van de Latijnse vertaling uit 1621 staat. De Arithmetica is een verzameling van dertien boeken waarin een reeks problemen van oplopende moeilijkheidsgraad wordt gegeven waarin naar rationale oplossingen gevraagd wordt. Diophantus geeft in alle gevallen wel een oplossing, maar niet de volledige oplossingsverzameling zoals we tegenwoordig graag willen. Van veel van de lastiger opgaven in de Arithmetica is nog steeds de volledige oplossing niet bekend. In deze voordracht zullen we daar een paar voorbeelden van laten zien. Daarna maken we een reuzensprong naar moderne tijden. De huidige hoeveelheid kennis over diophantische vergelijkingen is indrukwekkend, de vermoedens die erover bestaan zijn nog indrukwekkender. Zoals bijvoorbeeld de Vojta-vermoedens die een link leggen tussen de meetkunde van de vergelijking en de aard van de verzameling rationale punten.

Tegelijkertijd kunnen eenvoudige vragen echter niet beantwoord worden. Ook hier laten we een paar voorbeelden zien.
Tenslotte is er nog een stelling die min of meer zegt dat algemene diophantische vergelijkingen helemaal niet kunnen worden opgelost. Met deze onmogelijke uitdaging sluiten we de voordracht af.

De uitdagende vraagstukken van bedrijven

Dr. Vivi Rottschäfer

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

Tijdens de jaarlijkse Studiegroep Wiskunde met de Industrie komen ca. 50 wiskundigen bijeen om vraagstukken van bedrijven op te lossen. De wiskundigen komen uit heel Nederland samen om iets heel anders te doen dan zij normaal doen. Zij bestuderen tijdens deze week een vraagstuk van een bedrijf waarbij een wiskundige aanpak gevraagd wordt.
De afgelopen jaren werden er vraagstukken geformuleerd door KLM, KEMA, Marin, ESA, Stork, DSM, Rabobank en vele anderen.
De problemen zijn erg verschillend, daarom vergt het bestuderen van zo'n probleem een individuele aanpak waarbij gebruik gemaakt wordt van diverse wiskundige technieken. Daarbij weten de wiskundigen vaak weinig van het probleem af. Al met al is de Studiegroep Wiskunde met de Industrie elk jaar een leuke en uitdagende week waarin een eerste stap richting een oplossing voor een voor de wiskundigen niet alledaags probleem wordt gezet.

Hoe je het cryptosysteem RSA soms kunt kraken

Dr. Benne de Weger

Technische Universiteit Eindhoven
e-mail: b.m.m.d.weger@tue.nl

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 privésleutel. RSA maakt gebruik van eenvoudige getaltheorie en kan dan ook goed behandeld worden in een keuzeonderwerp Cryptografie bij Wiskunde D.

De veiligheid van de privésleutel moet natuurlijk gegarandeerd zijn. Deze sleutels worden bijvoorbeeld opgeslagen op smartcards, die niet zomaar uit te lezen zijn. Dat de privésleutel niet uit de bijbehorende publieke sleutel is af te leiden is gebaseerd op het feit dat het ontbinden van grote getallen in priemfactoren een erkend (maar onbewezen) moeilijk probleem is.
RSA heeft een goede reputatie als een zeer veilig systeem. Onder bepaalde omstandigheden is RSA echter wel degelijk te kraken. Gelukkig zijn deze omstandigheden makkelijk te vermijden, maar je wilt toch graag weten waar je aan toe bent. Enkele voorbeelden zullen de revue passeren. Als eerste kijken we naar zwakke sleutels. Met name de zogenaamde 'privé-exponent' moet niet te klein gekozen worden. We laten zien hoe kettingbreuken een rol spelen bij het kraken van RSA als deze privé-exponent te klein is, en hoe een geavanceerdere techniek daarin nog wat verder komt.
Deze techniek is het zoeken van kleine nulpunten van polynomen in twee variabelen. We zullen dit aan de hand van enkele voorbeelden illustreren.

Vervolgens gaan we uit van de omstandigheid dat een deel van de privésleutel gelekt is. Dat zou bijvoorbeeld kunnen door het stroomgebruik van de smartcard te meten terwijl die berekeningen doet met de privésleutel.
Als een voldoende groot deel van de privésleutel (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 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 privésleutel in zijn geheel kan lekken.

Voor wie zich een beetje wil inlezen: in de Vakantiecursus 2008 heeft Lenny Taelman de basis van RSA besproken, en in Euclides van juni en juli 2009 heb ik geschreven over zwakke sleutels bij RSA.

Rijen

Prof.dr. Arnoud van Rooij

Radboud Universiteit Nijmegen
e-mail: W.vandeSluis@math.ru.nl

Het is mijn bedoeling, u een paar onderwerpen voor te leggen die zich lenen voor één of twee uren in een klas. Er is een redelijke kans dat u, als ik ze noem, zult zeggen: `Dat kan niet; dat ligt ver boven het niveau; die man kent de school niet.'

Dat laatste is juist. Ik haal het ook niet in mijn hoofd om u uit te leggen hoe die onderwerpen in de klas behandeld moeten worden. Wat ik wél beweer is dat de moeilijkheden niet zitten in de materie zelf maar in een formalisme dat daar omheen gehangen wordt. Dat formalisme is nodig bij verdere studie, maar niet om het wezen van de zaak te zien.

Mijn eerste onderwerp is volledige inductie. U weet wat het is, en u weet ook dat de standaardverwoording problemen oproept. Volledige inductie betreft een fundamentele eigenschap van de natuurlijke getallen, en je zou redelijkerwijs kunnen denken dat die problemen tot de aard van het beest behoren. Welnu, ik neem op me, u te laten zien dat het niet zo is. Hoe volledige inductie werkt kun je aan doodsimpele voorbeelden laten zien; je moet alleen niet met een algemene formulering aankomen. (En wélke voorbeelden doodsimpel zijn kunt u beter uitmaken dan ik.)

Mijn tweede onderwerp gaat nog veel verder: de overaftelbaarheid van de reële getallen. Ik heb de ambitie, u te laten zien dat ook dát doenlijk is, zolang je je taal maar simpel houdt.

Cursusgeld

Het cursusgeld bedraagt €75, voor Eindhoven en voor Amsterdam, waarbij de syllabus en de maaltijden zijn inbegrepen.
Voor studenten aan lerarenopleidingen bedraagt het cursusgeld €25.

Aanmelding

Bij Minnie Middelberg per e-mail (Minnie.Middelberg@cwi.nl), via de website: http://www.cwi.nl/nl/Aanmelding_vakantiecursus_2010 of per post door het aanmeldingsformulier achterin de brochure in te vullen en op te sturen naar:

Centrum Wiskunde & Informatica
t.a.v. Minnie Middelberg
Postbus 94079
1090 GB Amsterdam

Tegelijkertijd dient men het cursusgeld over te maken op bankrekening 31.35.57.977 van de Stichting Wiskunde & Informatica Conferenties bij de RABObank te Amsterdam onder vermelding van uw naam en VC2010.

Onze buitenlandse gasten kunnen voor betaling gebruik maken van onderstaande gegevens.
BIC RABONL2U
IBAN NL76RABO0313557977

NB. Deze cursus geldt als nascholingsactiviteit
Voor geïnteresseerden is een nascholingscertificaat beschikbaar. Degene die daarop prijs stelt, gelieve dit bij aanmelding te laten weten door invulling en toezending van het formulier, achterin de brochure.

Plaats

Amsterdam: CWI, Science Park 123, Turingzaal.
Eindhoven: Auditorium TU Eindhoven, Den Dolech.

Syllabus

De syllabus zal worden uitgereikt bij aankomst op de cursus.

Informatie

Voor nadere informatie over de Vakantiecursus kunt u zich wenden tot Coby van Vonderen, tel. 020-592 4149, e-mail: Coby.van.Vonderen@cwi.nl .
Voor informatie over overnachtingen in Eindhoven kunt u contact opnemen met de VVV aldaar via het telefoonnummer 040-2979115 of via de beschikbare website http://www.vvveindhoven.nl/ .

Contacten Centrum Wiskunde & Informatica

Coby van Vonderen, 020 – 592 4149, e-mail: Coby.van.Vonderen@cwi.nl;
Minnie Middelberg, 020 – 592 4016, e-mail: Minnie.Middelberg@cwi.nl;
Centrum Wiskunde & Informatica, Science Park 123, 1098 XG; Postbus 94079, 1090 GB Amsterdam.

Docenten

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

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

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

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

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

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

Prof.dr. M. Sjerps, Nederlands Forensische Statistiek, Laan van Ypenburg 6, 2497 GB Den Haag, Korteweg-de Vries Instituut voor Wiskunde, FNWI Universiteit van Amsterdam, Postbus 94248, 1090 GE Amsterdam,
e-mail: m.sjerps@nfi.minjus.nl

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

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

Routebeschrijving

CWI

Met openbaar vervoer:

- Vanaf station Amsterdam Amstel en station Amsterdam Muiderpoort: bus 40 of bus 240. Zie www.gvb.nl voor meer informatie.
- Vanaf Amsterdam Centraal Station, of Almere, stopt er twee keer per uur een trein via station Muiderpoort op Science Park Amsterdam. Zie www.ns.nl voor meer informatie.
- Vanaf Amsterdam Centraal met tram 9 naar kruispunt Middenweg-Kruislaan en vandaar lopend over de Kruislaan naar het Science Park Amsterdam (ongeveer 1 km).

Met de auto:

Let op: In verband met werkzaamheden naar en op Science Park Amsterdam is een omleiding ingesteld om bij het Science Park te komen. Uw reistijd zal hierdoor, als u met de auto van de A10 komt, langer zijn dan gebruikelijk.

- Wanneer u uit de richting Amersfoort komt, neemt u de ring richting Utrecht/Den Haag.
- Wanneer u uit de richting Utrecht/Den Haag/Schiphol/Haarlem of Zaandam komt, neemt u de ring richting Amersfoort. Op de ring neemt u de afslag Watergraafsmeer/S113 (ring Oost). Aan het eind van de afrit volgt u de richting Science Park/Watergraafsmeer. U rijdt dan op de Middenweg.
- Volg vanaf de Middenweg de omleidingsborden naar Science Park Amsterdam, u komt dan vanzelf op de Carolina Mac Gillavrylaan. Via de rondweg van het Science Park zijn alle bedrijven en instituten te bereiken. Deze weg is tijdelijk éénrichtingsverkeer. Dit is aangegeven met borden en hekken.
- Aan cursisten die gebruik maken van een navigatiesysteem. De nieuwe straatnaam 'Science Park' is in veel systemen nog niet doorgevoerd. U kunt dan intoetsen: Kruislaan 413.

Parkeren: Sinds april 2010 is een parkeersysteem op het terrein van het CWI ingevoerd. Bij het oprijden moet u een parkeerkaart trekken. U ontvangt van de contactpersoon bij vertrek een uitrijkaart.

Technische Universiteit Eindhoven – Auditorium

Met openbaar vervoer:

- Alle universiteitsgebouwen liggen vlakbij het NS-station Eindhoven. U gaat de perrontrap af, dan rechtsaf en via de uitgang aan de noordzijde naar het busstation. U ziet de universiteitsgebouwen schuin rechts liggen op enkele minuten loopafstand. Op het TUE-terrein borden volgen naar ‘Auditorium’.

Met de auto:

- U rijdt Eindhoven binnen richting Centrum. Borden ‘Technische Universiteit’ volgen. U komt dan op de campus. Hier volgt u de borden ‘Auditorium’.

AANMELDINGSFORMULIER
VAKANTIECURSUS 2010
Wiskunde: de uitdaging

Ondergetekende,

Naam:

Functie:

Adres:

Postcode:

Woonplaats:

Telefoon:

E-mail:

wenst deel te nemen aan de Vakantiecursus 2010, die zal worden gehouden te

Amsterdam op vr. 27 en za. 28 augustus 2010 [ ]

Eindhoven op vr. 3 en za. 4 september 2010 [ ]

en heeft het verschuldigde bedrag van €75,- (dan wel €25,-) overgemaakt (voor rekeningnummers zie pagina 17).

Mijn voorkeur gaat uit naar vegetarisch eten [ ]

Nascholingscertificaat [ ]

Indien van toepassing, hier het adres van de onderwijsinstelling vermelden:

.....

Gelieve dit formulier vóór dinsdag 17 augustus 2010 te sturen naar:

Centrum Wiskunde & Informatica
t.a.v. Coby van Vonderen / Minnie Middelberg
o.v.v. Vakantiecursus 2010
Postbus 94079
1090 GB Amsterdam

NASCHOLINGSCERTIFICAAT
VAKANTIECURSUS 2010
Wiskunde: de uitdaging

Naam:

Voornamen (zonder afkortingen):

Geboortedatum:

Geboorteplaats:

Gelieve dit formulier vóór dinsdag 17 augustus 2010 te sturen naar:

Centrum Wiskunde & Informatica
o.v.v. Vakantiecursus 2010
t.a.v. Coby van Vonderen / Minnie Middelberg
Postbus 94079
1090 GB Amsterdam