Vakdidaktische achtergronden bij readers voor profielwerkstukken: "Kun je me de kortste weg vertellen?" en "Kun je de code kraken?"

Tuyp, M.M.C.

Award date:
2002

TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculteit Wiskunde en Informatica

AFSTUDEERVERSLAG

Vakdidaktische achtergronden

bij Readers voor Profielwerkstukken

"Kun je me de kortste weg vertellen?"

en

"Kun je de code kraken?"

door:
M.M.C. Tuyp

Afstudeerdocent: dr. A.G. van Asch
Juni 2002

Inhoud

1. Inleiding

Met ingang van augustus 1998 heeft ongeveer een kwart van de scholen in Nederland de 'tweede fase' ingevoerd voor de bovenbouw van het HAVO/VWO. In augustus 1999 is de 'tweede fase' bij de rest van de scholen in Nederland ingevoerd. Dit heeft consequenties voor het Hoger Beroepsonderwijs en het Wetenschappelijk Onderwijs. De nieuw instromende studenten uit deze 'tweede fase' zullen een andere manier van studeren gewoon zijn dan de studenten van voor de invoering van de 'tweede fase'. Met name om als universiteit goed voorbereid te zijn op deze nieuwe instroom, maar ook om de nieuwe studenten een idee te geven van wat ze kunnen verwachten op een universiteit is in september 1999 gestart met een aansluitingsproject VO-WO.

Dit aansluitingsproject is te splitsen in twee onderdelen, n.l.:

- Afstemming van het propedeuseonderwijs op de nieuw instromende studenten uit de 'tweede fase'
- Samenwerking met het voortgezet onderwijs op het gebied van hulp en ondersteuning bij praktische opdrachten, profielwerkstukken en oriëntatie op studie en beroepprojecten.

In het kader van het laatstgenoemde onderdeel is door enkele medewerkers en studenten van de faculteit Wiskunde en Informatica een aantal projecten ontwikkeld op het gebied van wiskundig modelleren, aansluitend op het examenprogramma van de wiskunde in de profielen N&G en N&T. Om deze projecten toegankelijk te maken voor docenten en studenten uit het voortgezet onderwijs is een internetsite opgezet waar ideeën voor praktische opdrachten en profielwerkstukken worden aangeboden, dan wel in html- of pdf-formaat. De wat grotere projecten in pdf-formaat zijn ook als boekje verkrijgbaar. Deze zijn voornamelijk bedoeld als onderwerpen voor profielwerkstukken en afgeleid van gegeven masterclasses uit de laatste jaren.

> Een profielwerkstuk is een uitgebreide praktische opdracht die elke leerling moet maken. In eerste instantie moesten twee vakken uit het profiel bij dit profielwerkstuk betrokken zijn, maar deze eis is bij de verlichtingsmaatregelen voor de studiedruk voor alle leerlingen die in 1999, 2000, 2001 en 2002 met de 'tweede fase' zijn begonnen komen te vervallen. Deze maatregel is een overgangsregeling: uiteindelijk zal toch moeten worden gestreefd naar tweevakkigheid. Het accent van het profielwerkstuk moet liggen op de vaardigheden en kennis die kenmerkend zijn voor het profiel. Het profielwerkstuk is een verplichte component in het examendossier, een leerling kan niet slagen als dit werkstuk niet met een voldoende is afgerond. Het is hierbij niet de bedoeling dat alleen het eindproduct wordt beoordeeld, ook het doorlopen proces dient door de leerling te worden gedocumenteerd en wordt in de beoordeling betrokken. De beoordeling van het profielwerkstuk heeft geen invloed op het examencijfer.

De masterclasses die door de TU/e worden gegeven zijn voornamelijk bedoeld voor de betere wiskunde leerlingen. De uitgegeven readers bij deze masterclasses zijn daarom niet direct geschikt als materiaal voor een profielwerkstuk, temeer omdat de mondelinge uitleg en de bij de masterclass gebruikte materialen niet beschikbaar zijn. Dit is een van

de redenen waarom is gekozen voor het uitbreiden en herschrijven van de readers van gegeven masterclasses. De andere reden voor het gebruiken van dit materiaal was de directe vraag naar onderwerpen voor profielwerkstukken van leerlingen en scholen en de beschikbaarheid van dit materiaal.

In dit verslag worden de implicaties die het omschrijven van de readers met zich meebracht beschreven. Verder wordt gekeken naar enige overeenkomsten met ZEBRAboekjes, de leerdoelen en de rol die de computer en grafische rekenmachine bij het verwerken van 'Kun je me de kortste weg vertellen?' en 'Kun je de code kraken?' kunnen spelen. Daarnaast is bij gebrek aan voldoende ervaringen met de boekjes 'Kun je me de kortste weg vertellen?' en 'Kun je de code kraken?' een hoofdstuk toegevoegd over ervaringen met profielwerkstukken in het algemeen. Hierbij is gebruik gemaakt van de ervaringen die bij het CITO bekend zijn uit de netwerkscholen die voor 1998 hebben proefgedraaid met het concept 'tweede fase'.

2. Transfer van Reader Masterclass naar Reader Profielwerkstuk

Hoewel de masterclasses op de TU/e worden georganiseerd voor alle leerlingen uit de bovenbouw van het VWO, zijn het toch over het algemeen de betere leerlingen uit de profielen N&G en N&T, met interesse voor een studie aan een technische universiteit die zich voor deze masterclasses inschrijven. Het niveau van de masterclasses is hierop aangepast. Het materiaal dat op zo'n dag wordt uitgereikt is niet een letterlijke weergave van alles wat tijdens de masterclass wordt verteld, maar een leidraad waar een verhaal bij hoort. Dit heeft als gevolg dat dit materiaal niet altijd door een gemiddelde leerling zonder enige vorm van begeleiding kan worden doorgenomen en begrepen om het vervolgens als basis voor het maken van een profielwerkstuk te gebruiken. De onderwerpen van de masterclasses op zich zijn echter wel geschikt als onderwerp voor profielwerkstuk. Het lag daarom voor de hand om het bestaande materiaal om te schrijven zodat dit kan worden gebruikt als instap voor het maken van een profielwerkstuk.

2.1 'Kun je me de kortste weg vertellen?'

De reader 'Kun je me de kortste weg vertellen?' is afgeleid van de Masterclass Combinatorische Optimalisering 'De kortste weg', gegeven op 5 maart 1999 door Prof. Dr. Jan Karel Lenstra en Dr. Ir. Cor Hurkens.

Een van de problemen die de begeleiders van de masterclass ondervonden was dat de hele slimme leerlingen de opgaven te makkelijk vonden terwijl de iets mindere leerlingen problemen hadden met het abstractieniveau van de reader. Daarnaast had ik zelf bij het doorlezen van de reader het gevoel dat het taalgebruik voor de doelgroep te formeel was. De vragen in de reader hadden te weinig diepgang voor een profielwerkstuk en het aantal opgaven was te weinig om een leerling werkelijk actief met de stof bezig te laten zijn. Aan de andere kant wilde ik ook niet te veel opgaven toevoegen omdat een reader voor een profielwerkstuk niet op een leerboek moet gaan lijken. Het is wel degelijk de bedoeling dat de leerling zelf ook het een en ander onderzoekt. Verder werden er in de uitleg soms nogal grote stappen genomen, waarvan ik aannam dat deze tijdens de masterclass waren verduidelijkt, maar die nu toch echt in de reader moesten worden vermeld. Verwijzingen zoals "We gaan ons vandaag bezighouden met..." moesten worden verwijderd.

De volgende veranderingen werden aangebracht:

- De inleiding werd uitgebreid en informeler geschreven. Zo werden de begrippen punten en kanten verduidelijkt met de begrippen knooppunten en wegen zoals die in het VO worden gebruikt. Het begrip **model** werd beschreven en opgaven 1 t/m 4 toegevoegd als zelfcontrole voor de daarvoor bestudeerde inleiding.
- In hoofdstuk 2 werden voorbeelden toegevoegd voor een klakkeloos ingevoerde c_{ij} en voor het begrip **circuit**.
- In de originele reader werd na het begrip circuit gelijk het Algoritme van Prim-Dijkstra gegeven. In de reader voor het profielwerkstuk is, om het geheel

geleidelijk op te bouwen, het 'Greedy' Algoritme met voorbeeld en bewijs toegevoegd. Naar aanleiding daarvan kunnen dan de opgaven 1 t/m 5 in paragraaf 2.3 gemaakt worden. Pas daarna heb ik laten zien dat een kleine aanpassing in het 'Greedy' Algoritme tot het Algoritme van Prim-Dijkstra leidt en ook daarbij een voorbeeld en opgaven toegevoegd.

- Hoofdstuk 3 begon in de reader van de masterclass direct met een abstracte uitleg van het kortste pad algoritme van Prof. Dijkstra. Ik heb enkele leerlingen in een 4VWO groep B1 dit stukje laten lezen. Zij hadden hier veel moeite mee. Bijna alle leerlingen probeerden het algoritme machtig te worden door de omschrijving toe te passen op een zelf verzonnen voorbeeld. Met dit in gedachten heb ik in de reader een dergelijk voorbeeld ingevoerd om het algoritme uit te leggen en de abstracte versie als samenvatting bijgegeven.
- Verder werd bij dit onderwerp tussen neus en lippen door vermeld dat het 'eenvoudig' was in te zien dat als in een stap alle tot dan toe bepaalde lengtes juist zijn, $L(k^*)$ dit ook is en dat voor het bewijs van deze bewering **volledige inductie** nodig is. Hierbij werd de 'eenvoudige' zienswijze niet geïllustreerd en werd het begrip 'volledige inductie' niet nader uitgelegd. Volledige inductie is een voor VO leerlingen onbekend begrip. De uitleg paste evenwel niet goed op deze plaats en is als bijlage toegevoegd. In opgave 5 bij dit hoofdstuk wordt nu gevraagd om met volledige inductie te laten zien dat met het beschreven algoritme inderdaad het kortste pad wordt gevonden. In de opgaven wordt als extra oefening ook een langste pad gevraagd.
- Het handelsreizigersprobleem werd in hoofdstuk 4 aan de orde gesteld. In tegenstelling tot de vorige hoofdstukken werden hier in de reader van de masterclass wel een zestal uitvoerige voorbeelden gegeven. Deze zijn onveranderd overgenomen.
- Bij de aannames die mogen worden gemaakt voor het zoeken naar een oplossing van een handelsreizigersprobleem wordt vermeld dat de afstanden moeten voldoen aan de **driehoeksongelijkheid**. Ook dit is voor VO leerlingen een niet bekend begrip. De omschrijving is echter triviaal en bovendien is dit een aardig simpel op te lossen probleempje voor de leerlingen zelf. Om deze reden is niet uitvoerig op dit begrip ingegaan.
- De uitleg over het aantal mogelijke routes is vervangen door een vraag. De leerlingen kunnen goed beredeneren dat het aantal routes $\frac{1}{2} \cdot (n-1)!$ is. Overigens wordt het begrip faculteit al in leerjaar 4 ingevoerd.
- De vragen die bij de verschillende algoritmes voor het benaderen van het optimum voor het handelsreizigersprobleem werden gesteld, zijn onder een apart hoofd gezet. De uitleg waarom de route die met het invoegingsalgoritme wordt gevonden korter is dan twee keer de kortste route is verwijderd. Dit probleem is als opgave gegeven.
- In het laatste hoofdstuk zijn een aantal opgaven uit het middagpracticum van de masterclass als gemengde opgaven gegeven. De opgaven waar verwijzingen naar internetpagina's zijn gegeven en waar gebruik werd gemaakt van het programma TRAVEL zijn weggelaten, daar deze tijdens de masterclass al problemen opleverden.

2.2 'Kun je de code kraken?'

De reader 'Kun je de code kraken?' is afgeleid van de Masterclass 'Informatiebeveiliging', gegeven op 22 maart 2000 door Prof. Dr. Henk C.A. van Tilborg.

Deze masterclass had een totaal ander karakter dan de masterclass 'Combinatorische Optimalisering'. De reader van deze masterclass bestond uit een in Mathematica vervaardigd Notebook. Deze zeer uitgebreide reader moest worden omgebouwd naar een papieren versie met voorbeelden en opgaven die met een rekenmachine goed te berekenen zouden zijn. In feite is dit een kleine verarming van het materiaal, maar Mathematica is te kostbaar en te geavanceerd om op middelbare scholen in te voeren.

Deze masterclass kende niet het probleem dat de opgaven te makkelijk werden gevonden en de taal te abstract. Integendeel de tekst van deze reader was heel goed te gebruiken alleen vergde hier het ombouwen van de opgaven, verbeteren van rekenfouten en het invoegen van getekende voorbeelden veel tijd.

De volgende veranderingen werden aangebracht:

- De inleiding bleef vrijwel gelijk op verwijzingen naar de masterclass na.
- In de inleiding van hoofdstuk twee werd de tekst iets gewijzigd. Bij de Vigenère tabel werd vermeld dat zijn naam niet echt bij deze tabel hoort. Hierna werd het modulo rekenen ingevoerd. Tijdens de masterclass werd met Mathematica gedemonstreerd dat:

  $20 + 10 \equiv 4 (\mathrm{mod}\, 26)$

  $6 \cdot 6 \equiv 10 (\mathrm{mod}\, 26)$

  $2^6 \equiv 12 (\mathrm{mod}\, 16)$

  Dit stuk is weggelaten alsmede de uitleg met voorbeelden dat in Mathematica eerst de letters nog naar een getalwaarde moest worden omgezet via de ASCII code. Als extra opgaven zijn wel toegevoegd het schrijven van een programmaatje dat tekst naar getallen omzet. Hierbij is dan nog de opmerking geplaatst dat dit eventueel kan worden vervangen door een zoektocht op het internet naar zo'n programmaatje. Deze zijn te vinden.
- Als extra oefening zijn wat simpele opgaven met modulorekenen toegevoegd. Dit was in de masterclass met het programma Mathematica voor de neus te triviaal geweest.
- Bij het onderwerp 'enkelvoudige substitutie' is het aantal mogelijke sleutels vervangen door de vraag hoeveel dit er zijn. Het voorbeeld waarin '*qnwtdwuzwgbymtqnwjfdamzsxwqqwdsagfqwhqofvwsaqlmfcxwqmcdwfvofgyfbdy pqmsysqwo*' met behulp van Mathematica moest worden vertaald naar '*the frequency of the various letters in a text makes it doable to break many a cryptosystem*' is vervangen door een opgave met dezelfde tekst die de leerlingen

zonder computer aanzienlijk meer tijd zal kosten om te ontcijferen. Dit laatste geldt zeker voor opgave 2.

- Ook bij het Vigenère systeem zijn de referenties naar Mathematica verwijderd. In de originele tekst werd een Vigenère code gebroken met behulp van een vercijferde tekst in Mathematica. Het bespreken zonder de hulp van het programma van dit proces zou te langdradig en verwarrend worden. In de reader voor het profielwerkstuk is daarom gekozen voor de uitleg van de '*Kasiski/Kerckhoff Methode*' . De internetlink is helaas verkeerd gekopieerd; het werkelijke adres is:
  http://www.cs.arizona.edu/people/math/Cipher/query_vcb.html. Deze link is nog steeds werkzaam. De code in opgave 1 is te kort om door het programmaatje op de gegeven link te laten oplossen. Hier moeten de leerlingen zelf aan de slag.
- In paragraaf 2.4 wordt de Enigma besproken. Het aantal lettervercijferingen dat nodig is om in de oorspronkelijke stand terug te keren wordt in de nieuwe reader als vraag gesteld, omdat het onderwerp tellen uitvoerig in klas 4 van het VO wordt behandeld. Het risico van het geven van internetlinks is natuurlijk dat deze na een tijdje opgeheven zijn. De hier gegeven links bestaan nog.
- De omzetting van 'klaretekst' naar een binaire string in Mathematica is in de paragraaf over blokcijfers vervangen door een korte beschrijving over hoe een tekst kan worden omgezet naar een binaire code. De uitleg over DES is vrijwel gelijk gebleven.
- Toen het boekje werd gedrukt was de ontwikkeling van AES bijna ten einde. In oktober 2000 werd door 'The Commerce Department' het volgende persbericht afgegeven:
  "A worldwide competition to develop a new encryption technique that can be used to protect computerized information ended today when Secretary of Commerce Norman Y. Mineta announced the nation's proposed new Advanced Encryption Standard.
- *Mineta named the Rijndael (pronounced Rhine-doll) data encryption formula as the winner of a three-year competition involving some of the world's leading cryptographers. "Once final, this standard will serve as a critical computer security tool supporting the rapid growth of electronic commerce," Mineta said. "This is a very significant step toward creating a more secure digital economy. It will allow e-commerce and e-government to flourish safely, creating new opportunities for all Americans," he said."*
  Het forum rond AES bestaat nog steeds.
- Onder het hoofdje identiteitscontrole is een korte tekst over smartcards tussengevoegd. De uitleg van de identiteitscontrole zelf is gelijk gebleven.
- In de paragraaf daarna is het stukje over 'triple DES' als extra informatie toegevoegd.
- In hoofdstuk 3 wordt verder in gegaan op de wiskundige principes achter het vercijferen. Dit hoofdstuk is bijna volledig herschreven. Het begrip ggd zou bij sommige leerlingen wel bekend kunnen zijn. De theorie erachter en het algoritme van Euclides is echter geen VO stof en dit vereist wat extra uitleg voordat de leerlingen aan het hoofdstuk over RSA kunnen werken. Het oefenen met wat simpele getallen maakt het geheel vaak wat sneller duidelijk.

- De kleine stelling van Fermat werd geïllustreerd met het voorbeeld $1234^{540} \equiv 1 (\mathrm{mod}\, 541)$. Dit is met Mathematica snel te laten zien, maar met de hand niet zo eenvoudig te berekenen. In de reader voor het profielwerkstuk is daarom gekozen voor wat simpelere voorbeelden i.e.: $2^4 \equiv 1 (\mathrm{mod}\, 5)$ en $10^6 \equiv 1 (\mathrm{mod}\, 7)$. Het 'bewijs' van de Stelling van Fermat is geen echt bewijs, omdat er met getallen wordt gewerkt. Het zou op een abstracte manier kunnen worden beschreven, maar dat maakt het voor de gemiddelde VO leerling niet erg duidelijk, dus is gekozen voor deze methode met de opmerking dat het bewijs voor andere a en p analoog verloopt.
- Bij het gedeelte over de Stelling van Euler zijn de Mathematicavoorbeelden verwijderd. Toegevoegd is een stukje over wat er gebeurd met getallen n die je niet als een vermenigvuldiging van slechts twee verschillende priemgetallen kunt schrijven en is $\phi(n)$ ingevoerd. Het invoegen van de Chinese Reststelling is achterwege gelaten, omdat dan teveel zou worden afgedwaald. Wel is een link naar een internetpagina over dit onderwerp gegeven. Om de extra gegeven stof in hoofdstuk 3 een klein beetje te oefenen zijn in paragraaf 3.3.1 zeven extra opgaven toegevoegd.
- De inleiding bij 'Machtsverheffen, worteltrekken en logaritmes nemen' is iets uitgebreid om duidelijk te maken wat er nu precies gedaan werd met de vraag 'bereken $6^{4371} (\mathrm{mod}\, 99991)$'. In de berekening $52331 \cdot 36151 \cdot 30198 \cdot 36 \cdot 6 \equiv 24455 (\mathrm{mod}\, 99991)$ staat een tikfout. Het antwoord moet zijn $34455 (\mathrm{mod}\, 99991)$. Verder is er een extra voorbeeld over modulorekenen met een aantal opgaven gegeven. Het grondidee van cryptosystemen met openbare sleutels is onveranderd gebleven.
- De gegeven link bij het RSA systeem http://www.math.princeton.edu/~arbooker/nthprime.html is niet opgeheven en kan nog worden gebruikt voor het generen van random priemgetallen. Op deze pagina kan ook de ϕ van het product van de gebruikte priemgetallen berekend worden. In de masterclass reader werd de ontcijferingsexponent met Mathematica berekend. In het profielwerkstukboekje wordt getoond hoe dit met gebruik van de stelling van Euler kan of met gebruik van de ggd van de vercijferingscode en de ϕ van het product van de gebruikte priemgetallen. Dit hoeft niet allemaal handmatig, ook de link http://www.math.sc.edu/~sumner/numbertheory/euclidean/euclidean.html is nog in bedrijf. Het 'echte' voorbeeld is alleen tekstueel aangepast om het gebruik van Mathematica te omzeilen.
- De paragraaf met de p-1 methode van Pollard is weggelaten omdat het voor het onderwerp van het profielwerkstuk niet echt relevant was.

Beide boekjes zijn niet bedoeld om als leerstof door te werken, de opgaven te maken en dan vervolgens als profielwerkstuk te worden beoordeeld. De stof beslaat ook niet de 80 slu die voor een profielwerkstuk moeten worden uitgetrokken. Ze zijn bedoeld om te proeven aan een onderdeel van de wiskunde waar dan verder zelf wat onderzoek in kan worden gedaan, met het boekje en de gegeven internetlinks als leidraad.

3. ZEBRAboekjes

Tijdens het schrijven van dit verslag werd mij de vraag gesteld of er een link kon worden gelegd tussen het maken van een profielwerkstuk en de ZEBRAblokken die in de lessen zijn ingepland. Hiertoe dient het begrip ZEBRAblok enige toelichting:

> In de diverse nieuwe wiskundeprogramma's van de VWO-profielen is een gedeelte met een omvang van 40 studielasturen gereserveerd voor keuzeonderwerpen, de zogenoemde ZEBRAruimte. In deze ZEBRAruimte wordt de leerlingen de gelegenheid geboden om zelfstandig of in (klein) groepsverband een of meerdere zelfgekozen onderwerpen te bestuderen en opdrachten uit te voeren die passen bij het gekozen profiel, de wiskunde in dat profiel en wellicht de toekomstige studie. De wiskunde in deze keuzeonderwerpen is niet een onderdeel van het reguliere programma, maar kan daar bovenuit stijgen, dan wel ernaast staan. Het moet een verrijking, een verbreding of verdieping van de leerstof zijn, doordat de wiskunde in een breder verband wordt geplaatst en de maatschappelijke relevantie van het vak helderder wordt gemaakt. De beperkte blik van de schoolwiskunde met de verplichte stof en de opgaven daarbij moet hierdoor worden verruimd. Het is de bedoeling dat de stof bijdraagt aan positieve beeldvorming van het vak wiskunde. Toetsing dient plaats te vinden binnen het schoolexamen.

Over het materiaal dat in een ZEBRAblok wordt bestudeerd, hoeft dus geen werkstuk te worden gemaakt. Het wordt wel op de normale wijze (d.m.v. een proefwerk o.i.d) getoetst. De meeste leraren kiezen er dan ook voor de hele klas dezelfde stof te laten bestuderen. Hiervoor zijn inmiddels verschillende boekjes uitgegeven door de NVvW en Epsilon Uitgaven, maar ook de verschillende methodes hebben eigen boekjes gedrukt.

Hoewel de readers 'Kun je me de kortste weg vertellen?' en 'Kun je de code kraken?' misschien in eerste blik iets op een ZEBRAboekje lijken, zijn beide boekjes daar niet echt voor geschikt en zou daar zeker qua opgaven een en ander aan moeten worden toegevoegd c.q. moeten worden veranderd. Mocht het zo zijn dat een docent er voor kiest om een van de readers als materiaal voor het ZEBRAblok te kiezen, dan kunnen de leerlingen dit materiaal niet meer als leidraad voor het profielwerkstuk nemen, omdat mijns inziens de onderwerpen van het ZEBRAblok en het profielwerkstuk van elkaar moeten verschillen. Is dit niet het geval dan moet een leerling al gelijk veel dieper op de stof ingaan om aan zijn of haar 80 SL-uren te komen. Naar verwachting zal dit voor de meeste leerlingen te moeilijk worden. De keuze moet derhalve òf ZEBRAblok òf profielwerkstuk zijn. Omdat zoals vermeld voor de ZEBRAblokken voldoende materiaal wordt aangeboden en de meeste leraren zich aan één onderwerp voor de hele groep houden om de werkdruk niet nog meer te verhogen, lijkt het dus meer zinvol om de readers beschikbaar te houden voor profielwerkstukken waar wel veel materiaal voor te vinden is, maar niet veel gestructureerd materiaal.

4. Leerdoelen

De leerdoelen die gekoppeld kunnen worden aan het maken van het profielwerkstuk zijn uitgebreid en divers. We hebben het immers over een 'meesterproef' waarin de leerling kan laten zien welke kennis hij of zij heeft opgedaan in zijn gehele studieloopbaan tot dan toe. De leerdoelen variëren van zeer algemeen via wat meer gespecialiseerd tot zeer specifiek voor het gekozen onderwerp. De onderverdeling ziet er dan als volgt uit.

4.1 Algemeen

In het examenprogramma van HAVO/VWO in de 'tweede fase' wordt aangegeven dat elke leerling 40 (HAVO) tot 80 (VWO) studielasturen moet besteden aan een profielwerkstuk dat qua inhoud kenmerkend moet zijn voor het profiel dat die betreffende leerling volgt. Dit werkstuk moet met voldoende of goed worden afgesloten. Het doorlopen proces moet in de beoordeling worden meegenomen, aldus:

> *Bij het profielwerkstuk wordt het doorlopen proces door de kandidaat gedocumenteerd (onderwerpskeuze, vraagstelling, verrichte werkzaamheden, geraadpleegde hulpbronnen en dergelijke). Dit wordt in de beoordeling betrokken. Voor de beoordeling van het profielwerkstuk wordt gebruik gemaakt van beoordelingscriteria die vooraf aan de kandidaat bekend gemaakt zijn.*

Om zo'n proces enigszins in de gaten te kunnen houden worden op mijn school, B.C.Broekhin, formulieren gebruikt (naar het voorbeeld zoals in de richtlijnen voor profielwerkstukken uitgegeven door het CITO) waarin een drietal beoordelingsmomenten wordt onderverdeeld in beoordelingsaspecten, zoals:

Beoordelingsmoment I:
- Heeft het onderwerp en de daarbij behorende (voorlopige) onderzoeksvraag een vakinhoudelijk niveau dat pas bij het schooltype (havo/vwo)?
- Heeft de leerling de (voorlopige) onderzoeksvraag opgesplitst in relevante vragen?
- Heeft de leerling bij de (voorlopige) onderzoeksvraag hypothesen opgesteld en/of verwachte uitkomsten of resultaten geformuleerd?
- Heeft de leerling een duidelijk realistisch plan van aanpak gemaakt?
- Geeft de opzet van het onderzoek antwoord op de (voorlopige) onderzoeksvraag en deelvragen?
- Heeft de leerling goed overzicht van geschikte informatiebronnen?
- In welke mate heeft de leerling zelfstandig gewerkt?

Beoordelingsmoment II:
- Wat is de informatieve kwaliteit van het logboek?
- Blijkt authenticiteit uit het logboek, het gesprek en de verzamelde informatie?
- Spoort het logboek met het plan van aanpak: met andere woorden ligt de leerling 'op schema'?
- Heeft de leerling geschikte informatiebronnen aangeboord en/of experimenten juist uitgevoerd en indien nodig de onderzoeksvraag bijgesteld?

- Heeft de leerling uit de informatiebronnen de relevante informatie gehaald c.q. zijn voldoende waarnemingen verricht en/of gegevens verzameld?
- Heeft de leerling de informatie geordend geschematiseerd en gestructureerd?
- Blijkt uit het logboek en de verzameld en bewerkte informatie dat de leerling de vakinhoudelijke problematiek en achtergrond begrepen heeft?
- Zijn de aanzetten tot conclusies uit de resultaten/bevindingen van het onderzoek verantwoord getrokken?
- In welke mate heeft de leerling zelfstandig gewerkt?

Beoordelingsmoment III (schriftelijk verslag):
- Hoe beoordeelt u de inleiding?
- Hoe beoordeelt u de hoofdtekst?
- Hoe beoordeelt u het slot?
- De techniek en de uiterlijke verzorging is...
- Het taalgebruik is...

Beoordelingsmoment III (mondelinge presentatie):
- Hoe beoordeelt u de inleiding?
- In welke mate geeft de leerling een uiteenzettend/betogend/beschouwend antwoord op de vraagstelling(en)?
- Hoe beoordeelt u de samenvatting/conclusie/aanbeveling?
- De techniek en de uiterlijke verzorging is...
- Het spreekgemak en de verstaanbaarheid is...

Het is natuurlijk niet noodzakelijk om strikt aan de hand van zo'n schema een leerling te beoordelen, maar het geeft wel een handvat. Belangrijk is dat de leerlingen moeten leren reflecteren op hun eigen leerproces. Ze moeten conclusies leren trekken in de trant van wat is juist/onjuist, volledig/onvolledig en aan de hand daarvan hun werk aanpassen.

4.2 Leren onderzoeken

De meeste leerlingen zijn niet elke dag met onderzoeksvragen bezig. Zij hebben hun lesboeken, bestuderen deze en maken de bijbehorende opgaven. Niemand zal zich met plezier verdiepen in een onderwerp dat hem of haar niet interesseert. Het is daarom belangrijk dat het onderwerp van het te maken profielwerkstuk in het interessegebied van de leerling ligt. Voor het leren onderzoeken kan worden gelet op de volgende onderdelen:
- De leerling moet zelf bepalen welk onderwerp voor hem/haar interessant is.
- Hij/zij moet zelf beslissingen nemen welke onderdelen van het gekozen onderwerp van belang zijn voor zijn/haar onderzoek.
- Het is van belang dat een leerling goed leert plannen.
- Hoe lost de leerling problemen op?
- Gaat hij/zij creatief met oplossingen en informatie om.
- Reflecteert de leerling tijdens het proces en reguleert hij/zij zichzelf?

4.3 Leren samenwerken

Niet alleen het zelfstandig kunnen werken maar ook het samenwerken met anderen is een onderdeel van het maken van een profielwerkstuk. In principe mag het profielwerkstuk individueel gemaakt worden, maar toch geniet het werken in groepjes de voorkeur omdat ook het leren samenwerken een onderdeel kan zijn van de opdracht en bovendien heeft het docententeam op die manier minder werkstukken te begeleiden. Op onze school werd gekozen voor groepjes van 2 à 3 personen. Het is daarbij wel een taak van de docent om in de gaten te houden dat niet al het werk op de schouders van één leerling wordt geladen of, wat ook gebeurt, dat één leerling al het werk naar zich toetrekt. Het is de bedoeling dat de leerlingen leren:

- Onderling tot een goede taakverdeling te komen,
- Elkaar te stimuleren
- Goede afspraken te maken
- Afspraken na te komen
- Overleggen
- Luisteren
- Communiceren en feedback geven
- Omgaan met verschillen
- Samen problemen op te lossen.

4.4 Zelfstandig leren werken

Een van de karakteristieken van de 'tweede fase' is de actieve en zelfstandige leerling. Deze karakteristiek is nodig om het te kunnen redden in het hoger onderwijs. Maar deze karakteristiek is ook meteen te gebruiken: met de vaardigheden die horen bij 'zelfstandigheid' moet een leerling ook beter in staat zijn zich de kennis en inhouden van diverse vakken eigen te maken.

Het profielwerkstuk doet een groot beroep op die zelfstandigheid. Bovendien is het profielwerkstuk één van de vier toetsonderdelen van het examendossier. Men kan zich daarom afvragen of een docent wel moet begeleiden en sturen. Uit ervaringen van de netwerkscholen bleek echter dat veel leerlingen begeleiding en sturing nodig hebben. Dit had diverse oorzaken. Sommige leerlingen hadden het zelfstandig werken nog niet goed onder controle. Anderen hadden een dusdanig moeilijk onderwerp, dat wel uitdagend en haalbaar was, mits er adequate begeleiding werd geboden. Daarbij is het voor de leerlingen waarschijnlijk de eerste keer dat zij zo'n grote opdracht moeten uitvoeren. Het profielwerkstuk is dan wel een toets, maar ook een leerproces en daarbij is begeleiding en sturing noodzakelijk.

4.5 Leren presenteren

Het eindproduct van het profielwerkstuk hoeft niet noodzakelijk een schriftelijk product in de vorm van een literatuurstudie of verslaglegging van een natuurwetenschappelijk onderzoek te zijn. Er kan ook worden gedacht aan werkstukken gemaakt op

ambachtelijk, technisch en/of kunstzinnig gebied. Het profielwerkstuk kent een breed scala aan mogelijke presentatievormen:

- Schriftelijke presentatie,
- Mondelinge presentatie met gebruik van media,
- Het product van een ontwerpopdracht,
- Een maquette,
- Een modeshow,
- Een toneeluitvoering,
- Een audio-, video-, foto- of (multimediale) computerpresentatie e.d.

Het is juist de bedoeling dat een profielwerkstuk bij voorkeur meer omvat dan een verslag van een literatuuronderzoek.

Al deze vaardigheden zijn vakoverstijgend en het is daarom belangrijk dat deze vaardigheden in onderlinge afstemming tussen vakken worden aangeleerd. Het kan niet de bedoeling zijn dat een wiskundedocent de leerling moet aanleren dat een verslag bestaat uit een index, inleiding, kern en slot. Dit zijn vaardigheden die bij de talen thuishoren, maar wel bij alle vakken moeten kunnen worden toegepast. Als dergelijke vaardigheden al niet vanaf het begin vakoverstijgend worden aangeleerd kan niet van een leerling worden verwacht dat hij of zij in staat zal zijn een vakoverstijgend profielwerkstuk te maken.

In dit kader spelen ook de ontwikkelingen in de informatie- en communicatietechnologie een grote rol. De ICT beïnvloedt immers de informatieverwerkingsvaardigheden, de tekstverwerkingsvaardigheden en de presentatievaardigheden, en juist deze spelen bij het maken van een profielwerkstuk een rol.

4.6 Leerdoel 'Kun je me de kortste weg vertellen?'

Het onderwerp 'Optimaliseren' met behulp van grafen wordt in het VO nauwelijks behandeld. De eerste keer dat leerlingen met grafen in aanraking komen is in een oppervlakkig hoofdstukje in de brugklas. Daarna in klas drie en vervolgens komt het onderdeel even aan de orde bij 'Grafen en Matrices' in 5VWO wiskunde A1 en A1,2. In de jaren 2002 en 2003 is 'Grafen en Matrices' geen onderdeel van het Centraal Examen A1 en A1,2 en staat het de docenten vrij om hierover vragen te stellen in de schoolexamens voor wiskunde A1 en A1,2. Voor de wiskunde B1 en B1,2 leerlingen komt het onderwerp na leerjaar 3 niet meer aan de orde.

Zoals eerder vermeld is het niet de bedoeling dat de leerlingen (of een docent) het doorwerken van het boekje zien als een profielwerkstuk op zich. Het is meer bedoeld als diepgaande informatiebron, een instap voor het onderzoeksonderwerp. Na het doorwerken van het boekje is het de bedoeling dat de leerlingen in ieder geval de volgende vaardigheden enigszins onder de knie hebben:

- Een leerling kan een simpel probleem vertalen naar een model.
- Een leerling kan een 'kortste boom' probleem oplossen.
- Een leerling kan een 'kortste pad' probleem oplossen.

- Een leerling kent enige algoritmes voor het benaderen van het optimum voor het handelsreizigersprobleem.
- Een leerling weet dat de optimale oplossing bij het benaderen van het optimum voor het handelsreizigersprobleem niet altijd kan worden gevonden en kan in eigen bewoordingen uitleggen waarom dit is.

Met deze vaardigheden zou de leerling op zoek kunnen gaan naar een probleem of puzzel. Hij/zij zou in een bibliotheek of op het internet op zoek kunnen gaan en zijn/haar bevindingen kunnen verwerken in een profielwerkstuk. Uiteraard kan het materiaal uit de reader en eventueel uitgewerkte opgaven als informatie worden bijgevoegd.

4.7 Leerdoel 'Kun je de code kraken?'

Cryptografie is, tenzij een leerling zich daar zelf heeft in verdiept, een onbekend onderwerp. Modulorekenen is onbekend. Daarentegen wordt wel uitvoerig ingegaan op exponentiële functies en logaritmen. Dit onderwerp kan als een uitbreiding op die stof worden gezien.

Deze reader heeft een iets moeilijker onderwerp dan het boekje 'Kun je me de kortste weg vertellen'. Zeker als een leerling alle opgaven maakt, waaronder ook het maken van kleine programmaatjes valt, is het de vraag of hij/zij al dusdanig diep met het onderwerp is bezig geweest en zoveel uren heeft besteed, dat bijna aan de eisen van een profielwerkstuk is voldaan. Hierbij moet dan wel een logboek worden bijgehouden en dienen de gemaakte programmaatjes te worden bijgevoegd, dan wel gedemonstreerd. Als een leerling niet alle opdrachten maakt zal net als bij het onderwerp 'Kun je me de kortste weg vertellen' een onderzoek moeten worden uitgevoerd. In de reader worden tal van interessante internetsites gegeven waar voldoende te vinden is. Na het doorwerken van de reader moeten de leerlingen:

- Enkele cryptosystemen kennen, hierover in hun eigen bewoordingen kunnen vertellen en het systeem eventueel aan een andere leerling kunnen uitleggen
- ggd van twee getallen kunnen bepalen
- Simpele modulo opgaven kunnen maken
- De kleine stelling van Fermat kennen
- De stelling van Euler kennen
- Euler ϕ kennen en de formule van Euler voor $\phi(n)$ kennen en kunnen uitleggen waarom dit zo is
- Het grondidee achter cryptosystemen met openbare sleutels kunnen uitleggen aan de hand van een simpel voorbeeld
- Iets kunnen vertellen over de veiligheid van RSA.

5. Rol van de computer/GR

De meeste wiskundedocenten vinden dat het computergebruik bij wiskunde zou moeten worden gestimuleerd, echter de beschikbare tijd om werkelijk iets met leerlingen te ondernemen ontbreekt vaak, afgezien van het niet beschikbaar zijn van juiste programma's. Een programma als Derive, Maple, of Mathematica is bijvoorbeeld op de school waar ik werk niet aanwezig. De leerlingen hebben de beschikking over de volgende programma's:

- Doorzien
- Excel
- Getal en Grafiek
- Grafen en Matrices
- PC-Calc (DOS)
- Ruimtemeetkunde (DOS)
- VU-Dynamo (DOS)
- VU-Grafiek
- VU-Stat
- Wcabri Geometrie

Toch kan met beperkte mogelijkheden veel worden bereikt en blijkt vaak dat de meeste leerlingen hier veel plezier aan beleven en zich daardoor meer voor het onderwerp interesseren.

5.1 Computer en GR bij 'Kun je me de kortste weg vertellen?'

In principe kunnen alle opgaven in deze reader zonder computer of grafische rekenmachine worden gemaakt, maar het onderwerp leent zich wel degelijk om ermee aan de slag te gaan met behulp van een computer. Op het internet zijn veel programmaatjes te vinden waarmee grafen kunnen worden gemaakt en bewerkt. De scholen die werken met de methode 'Getal en Ruimte' hebben de beschikking over het programma 'Grafen en Matrices' waar ook mee kan worden geëxperimenteerd. De GR tekent geen grafen, maar er kunnen wel bewerkingen op afstandenmatrices mee worden uitgevoerd. Op de site http://math.exeter.edu/rparris/ staan een negental gratis programmaatjes, waaronder het programmaatje windisc waarmee hele aardige bewerkingen op grafen kunnen worden uitgevoerd.

5.2 Computer en GR bij 'Kun je de code kraken?'

Tijdens de masterclass 'Kun je die code kraken?' werd veelvuldig gebruik gemaakt van het programma 'Mathematica'. Dit programma is echter voor de meeste scholen te kostbaar en de leerlingen moeten het daarom doen met Derive of soms zelfs alleen Excel en de standaardprogrammaatjes die bij de methodes worden meegeleverd. Toch heb ik ervoor gekozen om de leerlingen enkele programmaatjes te laten schrijven dan wel er naar te laten zoeken. Ook voor de problemen in deze reader is genoeg op het internet te vinden. Veel van de sites worden in de reader genoemd. Sommige bewerkingen kunnen aardig met de GR worden opgelost. Een klein programmaatje (voor de TI-83) om modulo te rekenen kan er bijvoorbeeld als volgt uitzien:

```
PROGRAM: MOD
: Prompt A,B
: A – int(A/B)*B → M
: Disp A, "MOD", B, "IS", M
: Delvar A
: Delvar B
: Delvar M
:
```

Ook het berekenen van een ggd hoeft met de GR geen probleem te zijn:

```
PROGRAM: GGD
: Prompt A,B
: A → X
: B → Y
: While B ≠ 0
: A – int(A/B)*B → C
: B → A
: C → B
: End
: Disp "GGD ", X, "EN ",Y, "IS",A
: Delvar A
: Delvar B
: Delvar C
: Delvar X
: Delvar Y
:
```

Overigens zijn veel functies in Excel te vinden, dus hoeft het oplossen van dergelijke opgaven een niet al te groot probleem te zijn.
Het omzetten van tekst naar cijfers gaat heel makkelijk in een programma als Excel waarin deze functie bestaat, als ook het omzetten van getallen naar tekst.

6. Tijdsbesteding

Het is moeilijk in te schatten hoeveel tijd aan de boekjes zal worden besteed door de gemiddelde leerling omdat ik daar niet genoeg gegevens over heb kunnen verzamelen. Gezien het feit dat een masterclass een hele dag in beslag nam en ik de readers heb uitgebreid met nogal wat extra opgaven, schat ik dat het doorwerken van de reader 'Kun je me de kortste weg vertellen' circa 16 uur in beslag zal nemen en de reader 'Kun je de code kraken' circa 20 uur.

7. Ervaringen met en door scholieren

De opdracht voor het schrijven van dit verslag werd mij 25 maart 2002 gegeven. Helaas hadden de leerlingen in de examenklassen in mijn school hun profielwerkstukken toen al afgerond en waren bezig met het schoolexamen onderdeel II. Daarna zouden zij nog één a twee weken naar school komen en 22 april 2002 de laatste lesdag hebben. Het was daardoor onmogelijk om daadwerkelijk zelf enige leerlingen te begeleiden bij het maken van een profielwerkstuk met behulp van de readers 'Kun je me de kortste weg vertellen?' en 'Kun je de code kraken?' Met dit in gedachten heb ik contact opgenomen met Jan Essers die mij enige namen kon geven van leerlingen die in het afgelopen jaar informatie over de betreffende onderwerpen hadden gevraagd. Op 26 maart heb ik per e-mail een formulier verstuurd naar een 10-tal leerlingen. 4 van de verzonden e-mails bleken niet bestelbaar. Van de andere 6 heb ik één reactie terugontvangen. Deze vindt u in de bijlagen.

Op onze school werd dit jaar voor het eerst met profielwerkstukken gewerkt. Veel docenten hadden het idee dat de leerlingen 'werkstukmoe' waren. Ze hebben in het voorgaande jaar al voor alle vakken een praktische opdracht moeten maken en zien het profielwerkstuk als niets anders dan nog zo'n praktische opdracht. Het idee dat dit werkstuk moet worden gezien als een soort meesterproef wil er niet echt in. Jammer genoeg werd deze houding ook nog lichtelijk gestimuleerd door enkele collega's die de leerlingen niet door het predikaat 'onvoldoende' de kans op slagen wilden ontnemen en dus boven een werkstuk, dat vaak niets anders was dan een aantal van het internet geplukte pagina's, een voldoende zetten. Natuurlijk is het ook zo dat na zo'n eerste jaar, waarvan we voor het overgrote deel van de scholen in Nederland toch kunnen spreken, nog weinig conclusies kunnen worden getrokken. Er waren nog veel vragen; vooral op organisatorisch gebied. Bovendien was voor veel collega's ook het beoordelen van een dergelijk werkstuk nieuw en kostte enige gewenning. Bij meerdere scholen is de aanpak van het geven van een vrije opdracht als praktische opdracht al gewijzigd. (Bijeenkomst aansluitingsproject VWO-WO 14 juni 2001 – zie bijlage -memo aan collega-docenten). Ik denk dat dit in de toekomst ook met de opdracht voor het profielwerkstuk zal gebeuren. Deze boekjes kunnen dan goed worden gebruikt door bijvoorbeeld een aantal opgaven verplicht in te laten leveren.

De leerlingen binnen onze school vonden vooral het geplande tijdstip voor het maken van het profielwerkstuk bezwaarlijk. De opdracht werd na de herfstvakantie gegeven en het geheel moest afgerond èn beoordeeld zijn voor 1 februari 2002. Gedurende die periode moest er ook gewerkt worden aan praktisch werk voor de vakken Biologie, Scheikunde en Natuurkunde en werden rond de Kerstperiode de Schoolexamens eerste periode gehouden. Toch valt er aan de keuze voor die periode weinig te veranderen. Het profielwerkstuk is een middel om de opgedane kennis en vaardigheden op hoog niveau te gebruiken om daarmee te laten zien dat een leerling *het profiel beheerst*. Eventueel zou het aanvangstijdstip kunnen worden vervroegd naar direct na de zomervakantie, maar veel eerder lijkt niet raadzaam. In het voorexamenjaar weet de leerling immers niet of hij of zij zal worden toegelaten tot het laatste jaar. Soms kiezen leerlingen ervoor om, indien zij het voorlaatste jaar niet halen, over te stappen naar een lagere

schoolvorm, i.e. van VWO naar HAVO of van HAVO naar VMBO. Als dan de leerling waarmee het werkstuk samen wordt gemaakt wel overgaat leidt dit tot problemen.

7.1 Ervaringen van netwerkscholen

Zoals beschreven in het onderdeel 'leerdoelen' is het de bedoeling dat het profielwerkstuk in etappes wordt beoordeeld. Een leerling kan pas aan het volgende gedeelte van zijn werkstuk beginnen als het voorgaande met voldoende of goed is beoordeeld. Daarna kan niet meer op dat deel van het werkstuk worden teruggekomen. Op deze manier zou er aan het eind van het proces altijd een voldoende of goed voor het profielwerkstuk moeten staan. Om die herkansing van gedeelten mogelijk te maken. kiezen de meeste scholen ervoor om de leerlingen in het voorexamenjaar met het profielwerkstuk te laten beginnen of direct bij de start van het examenjaar en de afronding rond de Kerstperiode te laten vallen. Er blijft dan voldoende tijd over voor eventuele uitloop voordat de examens beginnen.

Voorafgaande aan de begeleiding voor het maken van een profielwerkstuk moet worden aangegeven welke leerstof en vaardigheden horen bij het te maken werkstuk of over welke onderwerpen het werkstuk kan gaan. Daarbij moet de opdracht duidelijk worden omschreven. Van de leerling wordt geëist het onderwerp met de vraagstellingen duidelijk te omschrijven, tijdsplanning en de te gebruiken hulpmiddelen aan te geven en een logboek bij te houden. Verder moeten er duidelijke onderzoeksvragen geformuleerd worden en moeten besprekings- en beoordelingsmomenten worden vastgelegd. Als laatste is het de bedoeling dat de leerlingen van tevoren wordt verteld waarop ze zullen worden beoordeeld en hoe zo'n beoordeling tot stand komt. Een mogelijkheid om dit laatste te bewerkstelligen is om voor alle leerlingen een plenaire zitting te organiseren waarin een en ander wordt uitgelegd, waarna de leerlingen contact zoeken met de begeleidende docenten. Dit alles betekent een taakverzwaring voor een docent. Alles moet steeds meteen gecorrigeerd/beoordeeld of gelezen worden om de begeleiding optimaal te laten verlopen. Gebleken is dat het zeer noodzakelijk is om vaste afspraken in te roosteren. Het 'even tussendoor' helpen van leerlingen leidt tot inadequate hulp. Leerlingen moeten leren zich aan deze afspraken te houden. Helaas zijn bij veel scholen gestelde tijdslimieten soms fors overschreden, waardoor andere zaken in het gedrang kwamen. De inschatting van de benodigde tijd blijkt bij zowel leerlingen als docenten een groot knelpunt te zijn. Een tip uit de praktijk is om de geschatte tijd te vermenigvuldigen met een factor 2 en leerlingen nadrukkelijk te wijzen op de hoeveelheid werk die zij moeten leveren. Daarnaast zal in de toekomst extra tijd moeten worden uitgetrokken voor het overleg met collega's, als het profielwerkstuk weer vakoverschrijdend wordt. In de netwerkscholen is wel gewerkt met twee vakken voor het profielwerkstuk. Het overleg tussen secties en overleg met de andere begeleidende leraar nam verhoudingsgewijs heel veel tijd. Het begeleiden met twee docenten bleek ook moeilijk.

Een ander apart aandachtspunt vormen de presentaties. Hier stoppen leerlingen erg veel tijd in. Het is belangrijk dat de docent hiervoor beperkingen aangeeft om de tijdsdruk te verlagen.

Verder dient de docent de authenticiteit van het werk in de gaten te houden. In dit verband zijn het logboek en de tussentijdse besprekingen van groot belang. Desgewenst kan dan het traject worden aangepast door fases over te slaan of toe te voegen, extra materiaal aan te dragen of onderzoeksvragen te wijzigen. Het is handig om als docent zelf ook een procesverloop bij te houden. Bij geen of minder tussentijdse controles zijn de risico's op fraude groter. Gelukkig blijkt het aantal gevallen van (vermoede) fraude vooralsnog erg mee te vallen. Binnen het netwerk is tot nu toe één geval bekend en dat is nog in onderzoek. Scholen binnen het netwerk vrezen wel dat wanneer de tweede fase landelijk een aantal jaren draait het fraudeprobleem meer zal gaan spelen. Een manier om dit tegen te gaan is de leerlingen een gedeelte van de opdracht op school tijdens de lessen te laten maken.
Een aantal leerlingen van de netwerkscholen werd ondervraagd. Zij hadden vooral problemen met de eis van het bijhouden van een logboek. Dit vonden veel leerlingen slechts tijdverlies en het grootste gedeelte maakte vaak voor de besprekingen met de natte vinger een logboek. Een logboek zou alleen zinvol zijn bij het maken van proeven bij Biologie, Scheikunde of Natuurkunde. Het principe van beoordeling van het proces als het beoordelen van deelproducten is kennelijk nog niet duidelijk. De leerlingen waren wel te spreken over het zelf mogen kiezen van de opdracht en het zelf mogen werken. Als nadeel noemden zij dat ze toch de neiging hadden alles voor zich uit te schuiven waardoor ze veel dingen op het laatste moment moesten doen. Ook het mogen afwijken van de geijkte schriftelijke presentatievorm was voor sommige leerlingen een uitdaging.

8. Slot

In September 1999 is landelijk de tweede fase voor HAVO en VWO ingevoerd. Al in december 1999 hielden leerlingen een protestactie om de werkdruk te verlagen. In januari 2000 werden de volgende maatregelen doorgevoerd om scholen meer ruimte te geven bij het oplossen van invoeringsproblemen:

- De verplichte praktische opdrachten werden beperkt tot één per vak, de weging ervan werd aangepast.
- Het **profielwerkstuk** mocht betrekking hebben op één (deel)vak van het profieldeel.
- De scholen kregen de gelegenheid om binnen de examenprogramma's moderne vreemde talen1, CKV1 en ANW eigen keuze te maken: voorlopig hoefden niet alle eindtermen aan de orde te komen. Er werd sprake gemaakt van een ontwikkeltraject waarbij de individuele scholen de mogelijkheid kregen in maximaal drie jaar de studielast en de examenprogramma's in evenwicht te brengen. Dit zou moeten worden gevolgd door de inspectie en vakdeskundigen zouden hierbij betrokken worden. De genoemde (deel)vakken kregen net als voorheen alleen een schoolexamen, dat eerder mag worden afgerond dan in het laatste jaar. Dit zou ook gelden voor Frans1/Duits1 VWO.
- De examenverplichting in het vrije deel werd beperkt tot één (deel)vak.
- Voor scholen die al in 1998 met de tweede fase waren begonnen werd de uitslagregel aangepast, de VWO-scholen konden bovendien ter keuze van de school toepassing geven aan de eerste drie maatregelen en de HAVO-scholen konden een keuze maken ten aanzien van het **profielwerkstuk**.

De genoemde maatregelen gelden voor de leerlingen die in de jaren 1999, 2000 en 2001 zijn begonnen in leerjaar 4.
Toch bleken deze maatregelen niet voldoende. De bovengenoemde maatregelen werden verlengd tot 2002 en inmiddels zijn verschillende onderdelen in het examenprogramma geschrapt.

Wiskunde A1,2; Wiskunde B1 en Wiskunde B1,2 worden over het algemeen als overladen en moeilijk beschouwd. Zowel leerlingen als leraren ervaren de werkdruk als groot. Het lukt echter nauwelijks om voorstellen te krijgen voor onderwerpen die uit het programma verwijderd kunnen worden, omdat de samenhang tussen verschillende onderdelen dan verloren zou gaan. Juist de ruimte waarin wiskunde op een andere wijze geleerd zou kunnen worden, in de praktische opdrachten, het profielwerkstuk en de ZEBRAblokken, staat nu onder druk. In januari 2002 heeft Staatssecretaris Adelmund nieuwe voorstellen gedaan voor verandering van de huidige opzet van de Tweede Fase. Een groot gedeelte van deze aanpassingen kunnen pas in verband met wetswijzigingen per 1 augustus 2005 worden ingevoerd.

Er gaan stemmen op om de eenvakkigheid voor het profielwerkstuk te laten bestaan. Verder willen veel docenten dat tijd binnen het rooster wordt vrijgemaakt voor begeleiding en werken aan het profielwerkstuk binnen school. Omdat veel leerlingen en docenten het onbevredigend vinden dat er geen nuancering in de beoordeling van het profielwerkstuk kan worden aangebracht behalve voldoende of goed, wordt er ook regelmatig gepleit voor het becijferen van het profielwerkstuk.

Het (gedeeltelijk) meetellen van dit cijfer in het examencijfer zou een stimulans voor de leerlingen zijn om serieus onderzoek te verrichten.

Helaas bevinden de ontwikkelingen rond de tweede fase zich op dit moment in een impasse. Hierdoor dreigt een berusting te ontstaan, waartegen de gemotiveerde docent zich zou moeten verzetten. Het volgend jaar zal duidelijk worden of de doelstelling 'een betere aansluiting op de vervolgstudie' is behaald. Hopelijk zal een positief resultaat het onderwijs de positieve stimulans geven die de mogelijkheden van de tweede fase tot bloei zal laten komen.

Dankwoord

Graag wil ik iedereen die mij heeft geholpen bij het tot stand komen van dit verslag danken, waarbij ik de volgende personen speciaal even wil noemen:

- Bram van Asch, voor de bereidwilligheid om op het laatste moment in te springen als begeleider,
- Jan Donkers, voor de gedreven lessen en vele inspirerende gesprekken,
- Jan Essers, voor zijn collegialiteit en de namen van de leerlingen,
- Jan Karel Lenstra, voor het materiaal van het boekje 'Kun je me de kortste weg vertellen?'
- Hennie Ter Morsche, voor het regelen van vele zaken en de stimulans om door te gaan,
- Henk van Tilborg, voor het materiaal van het boekje 'Kun je de code kraken?' en zijn luisterend oor,
- Margaret Tjeerdsma (CITO), voor het prachtige materiaal dat zij mij geheel kosteloos ter beschikking stelde,
- Ed Moret (UU), voor de spreuk van Seneca

en als laatsten maar zeker niet de minsten:

- Frank van der Steen, voor zijn nimmer aflatende geloof in mij,
- mijn kinderen Peter, Alexander, Ian en Marjolein, voor het geduld met een niet altijd beschikbare moeder.

"*De beste wijze om iets te leren is er les in te geven.*" (Seneca)

TU/e, juni 2002

Informatiebronnen

Aansluiting VWO-WO TU/e
Centraal Instituut voor Toetsontwikkeling
Centrale Financiële Instellingen
Docentenhandleiding Profielwerkstukken 'B.C. Broekhin'
Nederlandse Vereniging voor Wiskundeleraren
Stichting Leerplanontwikkeling
Tweede Fase Adviespunt

Bijlagen

Vragenlijst
Memo aan collega-docenten
Tekst 'Kun je me de kortste weg vertellen?'
Tekst 'Kun je de code kraken?'
Docentenhandleidingen
Antwoordenboekjes

Vragenlijst				
Naam:	Stijntje Bokdam			
School:	Sint Ursula			
Profiel*:	C&M	E&M	N&G	N&T
	☐	☐	☒	☐
Schooljaar*:	4VWO	5VWO	6VWO	Anders, nl:
	☐	☐	☒	
Gekozen Opdracht*:	Kun je me de kortste weg vertellen?		Kun je de code kraken?	
	☐		☒	
Soort Werkstuk*:	Praktische Opdracht		Profielwerkstuk	
	☐		☒	
Gekozen vorm*:	Boekje gelezen en opdrachten gemaakt	Boekje gelezen en eigen werkstuk gemaakt	Anders, n.l.:	
	☐	☐	Boekje gelezen, opdrachten gemaakt en eigen werkstuk over priemgetallen en cryptologie gemaakt	
Hoeveel tijd heb je aan de opdracht besteed?	ongeveer 20uur			
Wat vond je van het niveau van het boekje?*	Te Makkelijk	Goed	Te Moeilijk	
	☐	☒	☐	
Ondervonden moeilijkheden bij de verwerking van het boekje:				
Waarom heb je dit onderwerp gekozen?	het leek me een heel interessant onderwerp en ik wilde graag mijn profielwerkstuk over wiskunde maken			
Heb je ooit een masterclass bezocht?*	Ja ☐	Titel:	Gegeven door:	Plaats:
	Nee ☒			
Verdere opmerkingen:				

* S.v.p. aankruisen wat van toepassing is.

B.C. Broekhin, 20 juni 2001.

Aan allen die met praktische opdrachten werken,

Donderdag 14 juni j.l. woonde ik een bijeenkomst bij waar afgevaardigden van een zestal scholen hun ervaringen met praktische opdrachten uitwisselden.

Alle aanwezigen hadden in eerste instantie dezelfde opzet gebruikt zoals wij die ook kennen. De leerlingen mochten een opdracht kiezen uit een aantal aangegeven hoofdstukken uit de methode en dienden deze voor een bepaalde datum uitgewerkt in te leveren.

De resultaten die hiermee werden behaald waren teleurstellend. Vaak zag het werk er nog wel goed verzorgd uit, maar de wiskundige inhoud was vrijwel nihil en de normering moest worden aangepast om nog enigszins redelijke cijfers te krijgen.

Enkele scholen besloten de aanpak te veranderen. De opdrachten werden gerichter. De volgende methoden van aanpak werden gebruikt (met betere resultaten):

1. De leerling kregen één opdracht ter voorbereiding. Vervolgens werden er twee middagen onder begeleiding (in de mediatheek) aan de praktische opdracht gewerkt die voor alle leerlingen gelijk was en die dezelfde dag ingeleverd moest worden. Niet af, dan elke dag te laat –1 punt.
   Voordelen: Makkelijker te normeren door gelijke opdracht. Het voortgangsproces was makkelijker te controleren.
   Nadelen: Deze opzet kost de inzet van twee leraren voor twee middagen die niet in het normale rooster waren opgenomen (dus eigen tijd!). De leerlingen hoeven niet zelf een onderwerp te vinden en worden een beetje naar een eindproduct gestuurd. Sommige groepjes keken bij andere groepjes af.
   Reacties: Veel leerlingen hadden moeite met het uitwerken van de opgaven binnen de beschikbare tijd, door kletsen e.d. en bij sommigen kwam er ondanks de instapopgaven weinig van de eindopdracht terecht. Degenen die het wel lukte waren heel tevreden; ze hadden een voldaan gevoel dat ze zelf iets hadden opgelost.
2. De leerlingen kregen een huiswerkopdracht die moest worden ingeleverd. Niet inleveren kostte punten. Daarna werd gezamenlijk een schoolopdracht gemaakt, die dezelfde dag werd ingenomen. Vervolgens kregen ze weer een huiswerkopdracht en na het op tijd inleveren van die opdracht volgde dan een uitgebreidere verwerkingsopdracht die ook thuis moest worden gemaakt. Bij de beoordeling ging 75% van de punten naar het product en 25% naar de verwerking. Ook hier kregen alle leerlingen dezelfde opdracht.
   Opmerkingen: Sommige leerlingen leverden de 1e huiswerkopdracht niet (op tijd) in. Dit kostte punten. Daarna werd er wel goed gewerkt. De huiswerkopdrachten en het schoolwerk werden over het algemeen redelijk tot goed gemaakt, maar de verwerkingsopdracht viel weer tegen.

3. De leerlingen kregen een gerichte opdracht waar ze 2 weken de tijd voor kregen om deze uit te werken.
   Voordelen: Als bij methode 1.
   De resultaten waren goed.
   Nadelen: Het werk lijkt erg op het gewoon maken van huiswerkopgaven die iets anders zijn geformuleerd en iets uitgebreider zijn dan in de methode.
4. De leerlingen kregen een gerichte opdracht waar ze enkele weken de tijd voor kregen, maar waar op school aan gewerkt moest worden en waarbij voor sommige onderdelen eerst goedkeuring van de docent moest worden gekregen, voordat verder kon worden gewerkt aan het vervolg van de opdracht.
   Commentaar: Als bij 3.

Andere opmerkingen die werden geplaatst waren:

- Leerlingen moeten tussentijds (wekelijks) het logboek laten zien, omdat de ervaring is dat dit pas achteraf met de natte vinger wordt gemaakt.
- Bij het zelf maken van opdrachten werden wiskundige namen opzettelijk veranderd zodat de leerlingen niet op het internet naar de uitwerking van hun probleem konden zoeken, maar echt zelf aan het werk moesten.
- Laat de leerlingen in groepjes om beurten een volledig hoofdstuk van de methode uitwerken zonder hulp van de docent en dit inleveren. (mtuyp: dit lijkt mij een minder goed idee)

Duidelijk is dat bovenstaande methoden meer van de leerkracht vergen, maar de resultaten zijn beduidend beter. (Er zouden eventueel hulpuren kunnen worden gebruikt om een en ander van de grond te krijgen.) Misschien is het een idee om i.p.v. een grote praktische opdracht twee kleinere opdrachten te laten maken. Eén onder begeleiding en de tweede zelfstandig, zodat de leerlingen weten wat er van hen wordt verlangd.

Het is uiteraard belangrijk om zeker de eerste jaren verschillende opdrachten voor handen te hebben; er zijn veel ideeën en voorbeelden van opdrachten op het internet te vinden.
www.tue.nl
www.stepnet.nl
www.math.rug.nl/betasteunpunt_opdrachten.nl

Als laatste voeg ik nog bij een opdracht die door B1,2 leerlingen van 5 VWO werd gemaakt en waar heel veel plezier aan werd beleefd. Dat moet toch een leuke stimulans zijn voor zowel leraar als leerling.

Groeten,
Marga Tuyp

Kun je die code kraken?

Inhoudsopgave

Informatiebeveiliging

30 augustus 2000

1 Beschermen van digitale gegevens

Dit boekje is een bewerking van de masterclass Informatiebeveiliging: "Kun je die code kraken?", gegeven op 22 maart 2000 door Prof.dr. Henk C.A. van Tilborg.

1.1 Inleiding

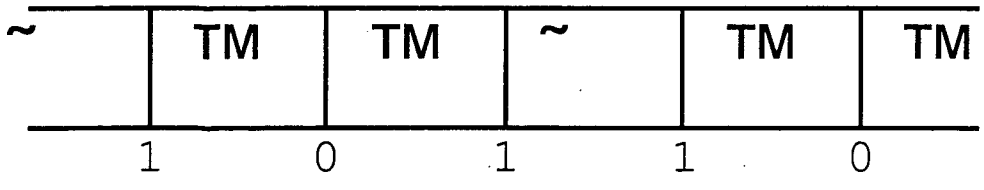
Vroeger werd informatie op veel verschillende manieren aangeboden en bewaard. Teksten en tekeningen stonden op papier en werden in archieven opgeslagen. Muziek op platen of nog eerder op een soort ponskaarten. Film en foto's worden opgeslagen als negatieven etc.

Tegenwoordig wordt bijna alle informatie digitaal opgeslagen en weergegeven. Digitaal wil zeggen dat de informatie is vertaald in lange rijen van nullen en enen. De reden is dat de moderne opslagmedia hiervoor heel erg geschikt is.

1.1.1 Voorbeelden van opslagmedia

1. Magnetische opslag, zoals op cassettebandjes, floppies en de harde schijf van een computer.

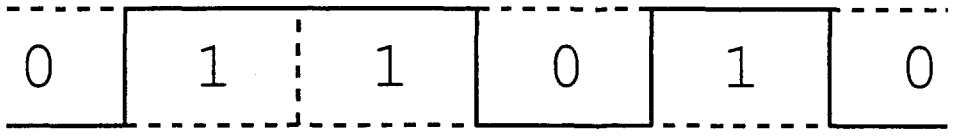
   Een floppy of harde schijf heeft sporen die in vakjes zijn verdeeld, waarin het magnetisch veld op twee manieren gericht kan worden: van links naar rechts of andersom. In de leeskop die de floppy of harde schijf moet 'lezen' zit een spoeltje. Hiermee kunnen wisselingen in het magnetisch veld worden geregistreerd en de informatie worden uitgelezen. Als het magnetisch veld in twee naast elkaar liggende vakjes dezelfde richting heeft wordt dit als een 0 geïnterpreteerd en als het magnetisch veld in een vakje de tegenovergestelde richting heeft als in het daarnaast liggende vakje, wordt dit als een 1 geïnterpreteerd.



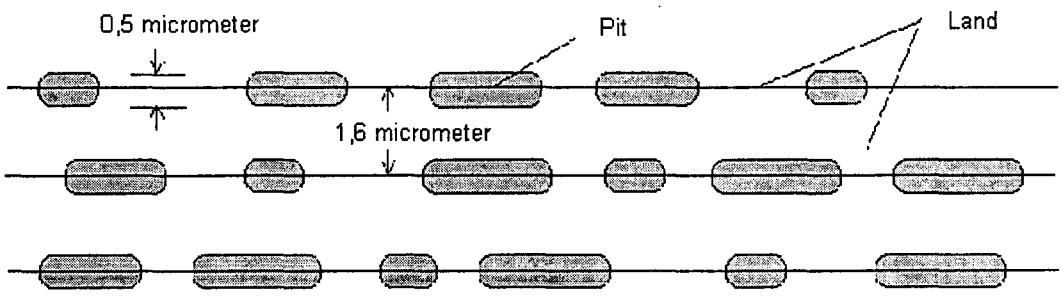
Figuur 1: Een spoor op een floppy of harde schijf.

2. Optische opslag, zoals compact disk, cd-rom.

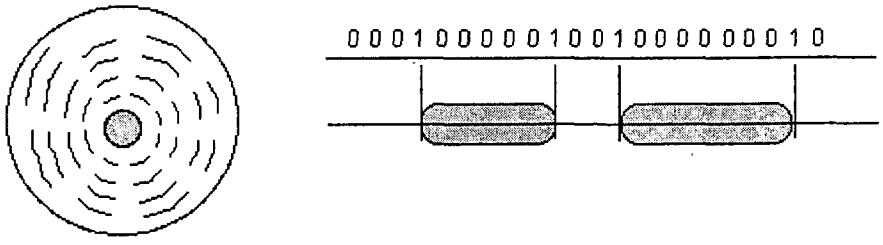
   Een cd-rom heeft ook sporen, die verdeeld zijn in stukjes. Deze stukjes worden wel of niet weggebrand. Er ontstaan dan putjes (in het Engels "pit" genoemd) en plateautjes (in het Engels "land") die nullen of enen aangeven. Met een laserstraal kan de informatie weer worden uitgelezen.



Figuur 2: Diepteprofiel van een spoor van een audio cd.



Figuur 3: De sporen op een cd sterk uitvergroot



Figuur 4: Binaire code van putjes

Een andere reden voor het digitaal opslaan van informatie is dat dit bij het versturen (zowel over draden als via draadloze verbindingen) interessante mogelijkheden biedt. Je kunt bijvoorbeeld met foutenverbeterende codes uit een verzwakt signaal het origineel weer volledig reconstrueren en dat zonodig weer doorsturen. (J.J. van Lint, Masterclass aan TUE in 1997.)

De vraag is welke garanties je uit veiligheidsoverwegingen wilt hebben op de digitale gegevens die je ontvangt en verstuurt? We denken aan:

1. **Geheimhouding**: iemand die door jou verstuurde gegevens onderschept of op je computersysteem binnendringt, moet die gegevens niet kunnen begrijpen.
2. **Handtekeningeigenschap**: de ontvanger van jouw boodschap wil graag een (digitaal) bewijs hebben dat die boodschap echt van jou komt. Dit bewijs zou een rechter moeten overtuigen.
3. **Integriteit**: de ontvanger van jouw boodschap wil graag een (digitaal) bewijs dat er niet met jouw boodschap geknoeid is.

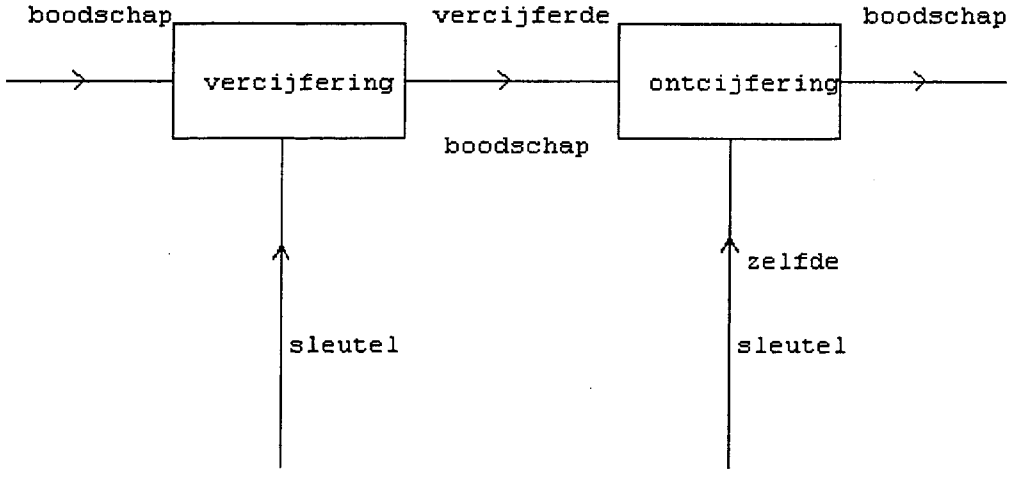
De moderne cryptologie probeert deze garanties via wiskundige methoden te realiseren.

2 Symmetrische cryptosystemen

Stel je wil een boodschap naar iemand versturen en je hebt afgesproken om de hele boodschap in een geheimschrift te vertalen (vercijferen) en de ontvanger van jouw bericht vertaalt het na ontvangst weer terug naar de goede boodschap (ontcijferen). Je moet dan wel allebei dezelfde geheimtaal kennen.

Meestal wordt in zulke gevallen gebruik gemaakt van standaard cryptografische methodes. De zender en de ontvanger moeten dan wel onderling een geheime *sleutelwaarde* hebben afgesproken om de vercijfering exclusief te houden. Anderen die wel dezelfde cryptografische methode gebruiken, kunnen dan toch niet die versleutelde berichten ontcijferen.

Dit noem je symmetrische cryptosystemen, omdat zender en ontvanger dezelfde sleutel hebben.



Figuur 5: Het schema van een symmetrisch cryptosysteem

2.1 Het Caesar cijfer

Het Caesar cijfer is genoemd naar Julius Caesar.

Julius Caesar leefde van 100 BC tot 44 BC. Hij leefde zowel op het persoonlijk vlak als in de politiek in een zeer vijandige omgeving. Hij werd op 15 maart 44 BC doodgestoken door een groep senatoren geleid door Brutus en Cassius.

Julius Caesar leefde dus in een moeilijke tijd en gebruikte daarom een vercijfermethode als hij boodschappen verzond. Deze methode werkt als volgt:

> Elke letter in het alfabet wordt cyclisch over k plaatsen verschoven. Met $k = 1$ wordt de *a* een *b*, de *b* een *c*, ... , en de *z* wordt weer een *a*. Met $k = 7$ en het woord *cleopatra* krijg je dan,

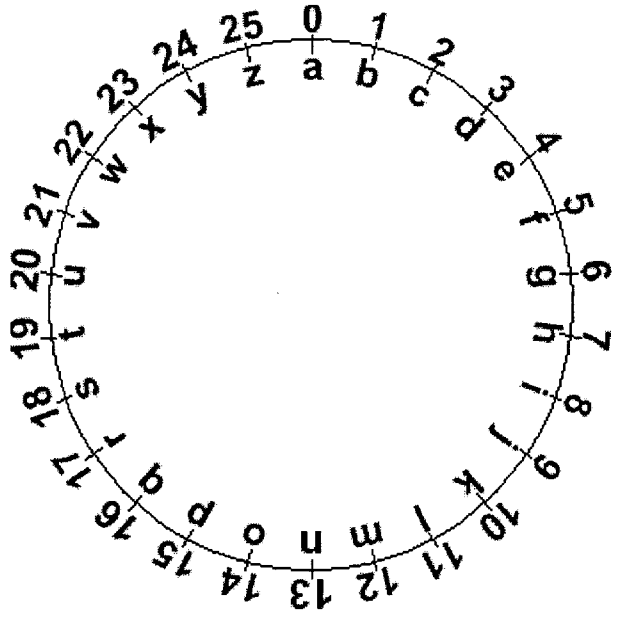
$$\textit{cleopatra} \xrightarrow{+1} \textbf{dmfpqbusb} \xrightarrow{+1} \textbf{engqrcvtc} \xrightarrow{+1} \textbf{folrsdwud} \xrightarrow{+1} \textbf{gpistexve} \xrightarrow{+1}$$
$$\textbf{hqjtufywf} \xrightarrow{+1} \textbf{irkuvgzxg} \xrightarrow{+1} \textit{jslvwhayh}.$$

> Zo'n optelling kun je ook met een Vigenère tabel uitvoeren. Blaise de Vigenère had een systeem om een beperkt aantal Caesar cijfers om de beurt toe te passen. Eigenlijk werkte hij aan een ingewikkelder systeem, maar door een foutje in de geschiedenis is zijn naam aan deze tabel blijven hangen.

0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Figuur 6: De Vigenère tabel

Je kunt het vercijferen met een Caesar cijfer ook door een computer laten uitvoeren. Je gebruikt dan een klokberekening. Op de klok staan de getallen 0,1,2, …, 25. De getallen stellen de letters *a* t/m *z* voor, dus 0 = *a*, 1 = *b*, …, 25 = *z*.



Figuur 7: Het alfabet op een klok met 26 cijfers.

Met ons voorbeeld *cleopatra* krijg je dan: $c + 7 = 2 + 7 = 9 = j$. Op dezelfde manier is $x + 7 = 23 + 7 = 30 = 4 = e$.

In de wiskunde heet klokrekenen modulo rekenen. Als je dus zegt dat je rekent *modulo* 26, dan werk je alleen met de getallen 0, 1, …, 25. Een uitkomst kleiner dan 0 of groter dan 25 bestaat niet. Als je een antwoord krijgt dat buiten {0,1, …, 25} ligt, dan moet je er net zolang 26 bij tellen of eraf trekken tot het antwoord weer binnen {0,1, …, 25} ligt. In plaats van = gebruik je bij het klokrekenen ≡ en zet je achter de uitkomst (mod "getal") om aan te geven dat je *modulo* een getal rekent. Dus:

> **$20 + 10 \equiv 4$ (mod 26), want 30 en 4 zijn hetzelfde modulo 26,**
> **$6 \times 6 \equiv 10$ (mod 26), want 36 en 10 zijn hetzelfde modulo 26,**
> **$2^6 \equiv 12$ (mod 26), want 64 en 12 zijn hetzelfde modulo 26, m.a.w. 2^6 en 12 verschillen een veelvoud van 26 van elkaar. (Op de cirkel zijn ze hetzelfde.)**

Je kunt zeggen dat je bij elke berekening het antwoord deelt door 26 en dat je de rest neemt. Dit noem je *reduceren* modulo 26. Er zijn computerprogramma's die heel snel *modulo* kunnen rekenen.

Een Caesar vercijfering is echter heel simpel te breken door alle sleutels uit te proberen. In het Engels heet deze methode "Exhaustive key search". Je neemt dan gewoon een stuk vercijferde tekst, trekt elke mogelijke sleutelwaarde 0, 1, …, 25 ervan af en kijkt welke sleutel een stuk Nederlandse tekst oplevert.

0	vvrnpqiybabz
1	uuqmophxazay
2	ttplnogwzyzx
3	ssokmnfvyxyw
4	rrnjlmeuxwxv
5	qqmikldtwvwu
6	pplhjkcsvuvt
7	ookgijbrutus
8	nnjfhiaqtstr
9	mmieghzpsrsq
10	llhdfgyorqrp
11	kkgcefxnqpqo
12	jjfbdewmpopn
13	iieacdvlonom
14	hhdzbcuknmnl
15	ggcyabtjmlmk
16	ffbxzasilklj
17	eeawyzrhkjki
18	ddzvxyqgjijh
19	ccyuwxpfihig
20	bbxtvwoehghf
21	aawsuvndgfge
22	zzvrtumcfefd
23	yyuqstlbedec
24	xxtprskadcdb
25	wwsoqrjzcbca

2.1.1 Opgaven

1. Vercijfer de tekst "profielen" met het Caesar cijfer als de sleutel het getal 20 is.
2. Welke sleutel is gebruikt in de Caesar vercijfering "gyymnylefum"?
3. Bereken:
   a) 237 (mod 11)
   b) 1496 (mod 9)
   c) -401 (mod 7)
4. * Maak zelf een programmaatje waarmee je tekst in getallen kunt omzetten en weer terug.
5. * Maak zelf een programmaatje waarmee je modulo kunt rekenen.
6. * Maak een programmaatje dat met behulp van de Caesarcode teksten vercijfert en ontcijfert.

* Deze opgaven kunnen desgewenst worden overgeslagen of vervangen met de opdracht zo'n programmaatje op het internet te zoeken.

2.2 Enkelvoudige substitutie

2.2.1 Het systeem

Een andere mogelijkheid om teksten te vercijferen is elke letter uit het alfabet door een vaste andere letter van het alfabet te vervangen. Bijvoorbeeld:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
k	h	y	l	z	j	f	c	b	w	t	r	n	a	e	v	x	o	g	q	m	p	u	d	s	i

Een "Exhaustive key search" is hier niet aan te raden.

Vraag: Hoeveel mogelijke sleutels heb je bij dit systeem?

2.2.2 Veiligheid van enkelvoudige substitutie

Als je de vraag in 2.2.1 hebt kunnen beantwoorden krijg je misschien het vermoeden dat dit systeem veilig is. Dit is niet zo! De reden hiervoor zijn de kansverdelingen in een taal. In het Engels hebben de individuele letters bijvoorbeeld de volgende kansverdeling:

a	0.0804	h	0.0549	o	0.0760	v	0.0099
b	0.0154	i	0.0726	p	0.0200	w	0.0192
c	0.0306	j	0.0016	q	0.0011	x	0.0019
d	0.0399	k	0.0067	r	0.0612	y	0.0173
e	0.1251	l	0.0414	s	0.0654	z	0.0009
f	0.0230	m	0.0253	t	0.0925		
g	0.0196	n	0.0709	u	0.0271		

Figuur 8: Kansverdeling van letters in een Engelse tekst.

Als je dus alle letters *e* vervangt door een *z*, dan zal 12,5% van de letters in de vercijferde tekst gelijk zijn aan *z*. En als *t* is vervangen door een *q* dan zal 9% van de letters in de vercijferde tekst een *q* zijn. In feite hoef je dus alleen maar (een voldoende groot gedeelte van) de tekst te turven.

2.2.3 Opgaven

1. De volgende vercijferde tekst is een Engelse zin. Het totale aantal tekens is: 75.

   "qnwtdwuzwgbymtqnwjfdamzsxwqqwdsagfqwhqofvwsaqlmfcxwqmc dwfvofgyfbdypqmsysqwo"

   Ontcijfer de tekst.

2.3 Het Vigenère systeem

2.3.1 Het systeem

Bij het Vigenère systeem wordt een beperkt aantal Caesar cijfers om de beurt toegepast. Dit gebeurt aan de hand van een sleutelwoord. Bijvoorbeeld als het sleutelwoord "mus" is, dan pas je de Caesar cijfers met waarde 12, 20 en 18 om de beurt toe.

```
i s e e n m e e s t e r k l a s e e n k l a s m e t e e n
m u s m u s m u s m u s m u s m u s m u s m u s m u s m u
u m w q h e q y k f y j w f s e y w z e d m m e q n w q h
```

Je kunt bij de vercijfering de Vigenère tabel uit figuur: 6 op blz. 8 gebruiken.

2.3.2 Gevallen van toeval

We hadden al gezien dat de Caesar vercijfering heel makkelijk te breken is en ook enkelvoudige substitutie van letters geen veiligheid kan garanderen. Op dezelfde manier kun je met behulp van kansen inzien dat de lengte van een Vigenère sleutel te achterhalen is en het dan verder niet meer zo moeilijk is om de vercijfering te breken.

De kans dat twee willekeurige letters in een Engelse tekst hetzelfde zijn is niet $1/26 \approx 0{,}0385$, maar gelijk aan de kans dat ze alle twee gelijk zijn aan de letter *a* plus de kans dat ze alle twee gelijk zijn aan de letter *b*, etc. Met de tabel in figuur 8, vindt je dan dat die kans gelijk wordt aan:

$$(p(a)^2) + (p(b))^2 + \ldots + (p(z))^2 = 0.804^2 + 0.0154^2 + \ldots + 0.0009^2 \approx 0.06875.$$

Stel nu eens dat je een vercijfering hebt gemaakt met het Vigenère systeem en je hebt een sleutelwoord gebruikt van lengte 3. Als nu twee letters in je oorspronkelijke tekst hetzelfde zijn èn 3 plaatsen van elkaar verwijderd zijn, dan zijn die letters in je vercijfering ook hetzelfde. Dit geldt natuurlijk ook als ze 6 plaatsen van elkaar staan, of 9, of 12, enz.

Als twee letters op *l* posities van elkaar verwijderd zijn en *l* niet een veelvoud is van 3, dan is de kans dat twee overeenstemmende symbolen in de vercijferde tekst gelijk zijn aan elkaar 1/26. (Als de sleutel willekeurig gekozen is).

Kijk maar eens naar de eerdere vercijfering:

```
i s e e n m e e s t e r k l a s e e n k l a s m e t e e n
m u s m u s m u s m u s m u s m u s m u s m u s m u s m u
u m w q h e q y k f y j w f s e y w z e d m m e q n w q h
```

Nu neem je de cijfertekst en verschuif die over drie plaatsen. Tel vervolgens het aantal overeenkomsten. Je ziet drie "toevallige" overeenkomsten op 26 vergelijkingen. Dat is dus $3/26 \approx 0{,}115$. Dit is meer dan 0,06875, maar nog veel meer dan 1/26. Als je de cijfertekst over 4 plaatsen verschuift dan zie je dit niet.

u m w q h e q y k f y j w f s e y w z e d m m e q n w q h
u m w q h e q y k f y j w f s e y w z e d m m e q n w q h

2.3.3 Het breken van een Vigenère Code

De Kasiski/Kerckhoff Methode

Vigenère-vercijfering werd ongeveer 300 jaar lang als vrijwel onbreekbaar beschouwd, maar in 1863 bedacht een Pruisische Majoor, Kasiski een methode die bestond uit het vinden van de lengte van de sleutel. Zodra de lengte van de sleutel is achterhaald is het simpel om de vercijferde boodschap in precies dat aantal enkelvoudige substituties te splitsen en in paragraaf 2.2.2 heb je kunnen zien dat deze vrij simpel te breken zijn. De techniek die Kasiski gebruikte om de lengte van een sleutel te vinden is gebaseerd op het bepalen van de afstand tussen de herhaling van twee letters die steeds naast elkaar staan. Kijk eens naar de volgende vercijferde tekst.

KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

KS komt twee keer voor, beginnend op positie 0 en positie 9.

KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Het tweetal ME komt ook twee keer voor, beginnend op positie 2 en positie 11.

Nu is het voorbeeld hier erg klein. Deze methode werkt beter met grotere teksten, waarin je zult zien dat zulke herhalingen vaak voorkomen en hoewel niet elke herhaling een gevolg van de sleutel hoeft te zijn, zullen de meeste herhalingen toch de basis leveren voor het breken van de sleutellengte door de afstand te meten tussen de herhalingen van de tweetallen letters, in dit geval 9.

Kasiski maakte dan de volgende tabel:

Tweetal	Plaats	Afstand	Factoren
KS	0, 9	9	3, 9
SM	1,10	9	3, 9
ME	2, 11	9	3, 9

Het factoriseren van de afstanden tussen herhaalde tweetallen is een manier om mogelijke sleutellengtes te bepalen. De factoren die het meest voorkomen zullen de meest waarschijnlijke sleutellengte opleveren. In dit geval is er geen voorkeur. (N.B. Bij langere teksten zullen ook meervouden van 9 als factor tevoorschijn komen. Deze hebben ook 3 als factor.)

Zodra de lengte van een sleutelwoord bekend is (hier 9) kan de tekst worden opgesplitst in precies zoveel substituties. Elke 9^{de} letter is vercijferd met dezelfde sleutelletter. Kasiski gaat dan verder met het analyseren van de frequentie en andere standaard technieken om een enkelvoudige substitutie te ontcijferen.

Een variant op deze methode werd voorgesteld door de Franse cryptograaf Kerckhoff. Deze probeert het sleutelwoord zelf te vinden en vervolgens de vercijferde tekst te ontcijferen. Hij verdeelt de boodschap in kolommen die corresponderen met de enkelvoudige susbstitutie, turft vervolgens de frequenties in elke kolom en gebruikt deze en logische analyse om de sleutel te construeren. Stel dat bijvoorbeeld de meest voorkomende letter in de eerste kolom de letter 'K' is, dan zou je kunnen zeggen dat 'K' overeenkomt met 'E'. Met de Vigenère tabel op blz. 6 kun je dan aflezen dat de eerste letter van de sleutel de letter 'G' moet zijn.

Het probleem met deze 'handmatige' aanpak is dat er in korte boodschappen verschillende letters als kadidaat voor de letter 'E' voorkomen en je dus de verschillende mogelijkheden moet nagaan. Tegenwoordig maakt men gebruik van de chi-kwadraat toets om vast te stellen welke van de 26 mogelijke verschuivingen voor elke letter van het sleutelwoord is gebruikt.

Een (door jezelf) vercijferde code van meer dan 150 karakters kun je invoeren op:
http://www.cs.arizona.edu/http/html/people/muth/Cipher/query_vcb.html

2.3.4 Opgaven

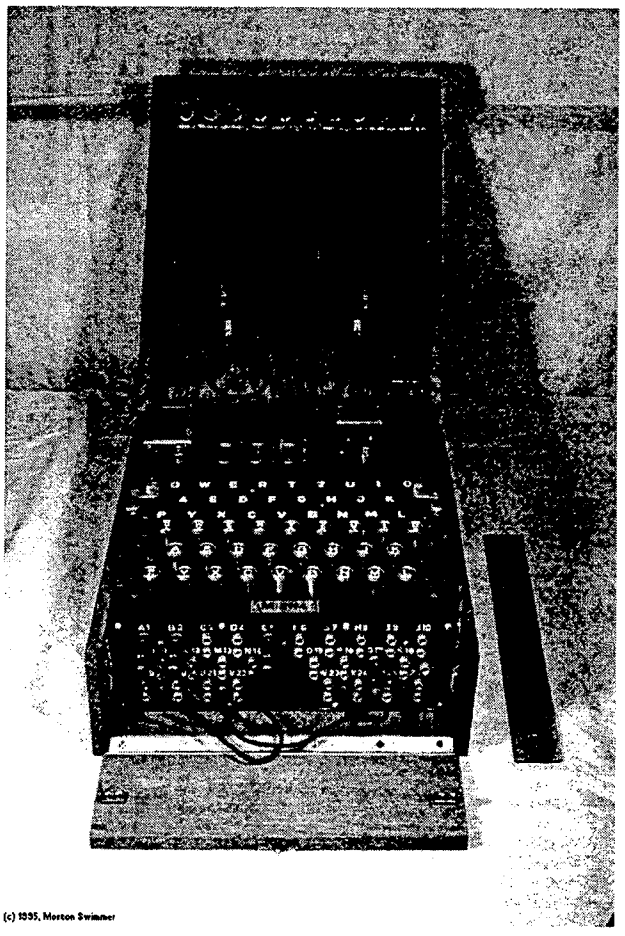
1. Probeer de tekst `KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY` te ontcijferen. Je mag aannemen dat de sleutel 9 karakters lang is en verder is gegegeven: 'K_1' = 'T' en 'S_1' = 'O'. Welke sleutel is gebruikt?
2. * Ontcijfer de volgende code:

```
ANYVG YSTYN RPLWH RDTKX RNYPV QTGHP HZKFE YUMUS AYWVK ZYEZM
EZUDL JKTUL JLKQB JUQVU ECKBN RCTHP KESXM AZOEN SXGOL PGNLE
EBMMT GCSSV MRSEZ MXHLP KJEJH TUPZU EDWKN NNRWA GEEXS LKZUD
LJKFI XHTKP IAZMX FACWC TQIDU WBRRL TTKVN AJWVB REAWT NSEZM
OECSS VMRSL JMLEE BMMTG AYVIY GHPEM YFARW AOAEL UPIUA YYMGE
EMJQK SFCGU GYBPJ BPZYP JASNN FSTUS STYVG YS
```

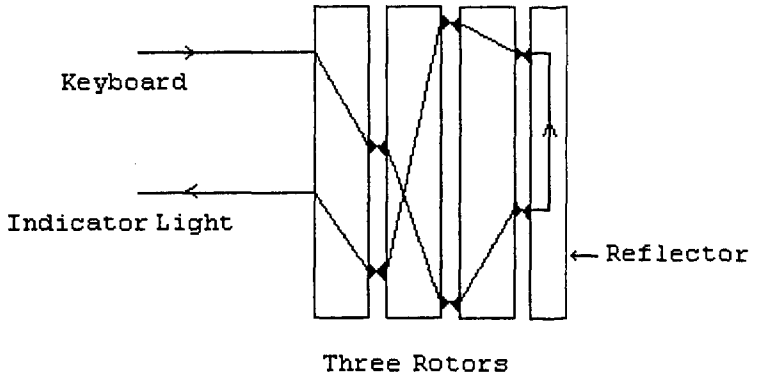
* Deze opgave is pittig en kan desgewenst worden overgeslagen.

2.4 Enigma

De Enigma is een vercijferingsmachine die in de Tweede Wereldoorlog door de Duitsers werd gebruikt.



De Enigma heeft een gewoon toetsenbord voor de letters *a, b, ..., z.* Daarboven zie je nog eens de 26 letters van het alfabet, maar dan met lampjes eronder. Helemaal bovenin zie je 3 schijven en een zogenaamde reflector. Iedere schijf heeft aan beide platte kanten 26 contactpuntjes. Binnen de schijf zijn die op een willekeurige manier verbonden (de Duitsers hadden ongeveer tien verschillende schijven). Als je een letter intoetst, gaat er een stroom naar het contactpunt van de eerste schijf. Die stuurt het op een andere plaats door naar de tweede schijf en die stuurt het op weer een andere plaats door naar de derde schijf. Deze schijf geeft het door aan de reflector, die het stroompje via een ander contactpunt weer terugstuurt. De schijven worden dan dus in de omgekeerde volgorde nog eens doorlopen. Uiteindelijk gaat er een lampje branden, wat de vercijfering van de ingetoetste letter aangeeft.



Figuur 8: Een schematische weergave van de Enigma

Na elke toetsaanslag draait de meest linkse schijf één positie door. Dat betekent dat een tweede vercijfering van dezelfde letter een andere vercijfering oplevert. Na 26 keer doorschuiven van de linkse schijf (dus één keer rond), zal de tweede schijf één positie meeklikken (zoals bij een kilometerteller na elke 10 km). Als de middelste schijf 26 klikken heeft gemaakt, draait ook de derde schijf één positie verder. De reflector beweegt niet.

Vraag: Na hoeveel letterver cijferingen is de machine terug in de oorspronkelijke stand?

De vercijferringsleutel bij deze machine is hetzelfde als de ontcijferingssleutel. Zender en ontvanger moeten van tevoren afspreken welke schijven ze gaan gebruiken, in welke volgorde ze staan en wat hun positie is.

De Engelsen konden veel boodschappen van de Duitsers ontcijferen. Dit was veel werk, want de sleutel was niet bekend. Alan Turing, die later een wereldberoemd informaticus werd, heeft veel gedaan voor de ontcijfering van Enigma boodschappen. Een artikel over het breken van de Enigma codes kun je vinden op:

http://www.cl.cam.ac.uk/Research/Security/Historical/azzole1.html
(ULTRA: THE SILVER BULLET
Breaking the German Enigma Codes
By Pete Azzole)

Andere interessante sites zijn:
http://www.math.arizona.edu/~dsl/enigma.htm
http://raphael.math.uic.edu/~jeremy/crypt/enigma.html
Veel foto's van de machine kun je vinden op:
http://www.math.arizona.edu/~dsl/ephotos.htm
Een java applet met een simulatie van een werkend model van de enigma vind je op:
http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/

Vraag: De Duitsers dachten dat het aanbrengen van de reflector in het ontwerp veel voordelen zou hebben. Zie je ook een nadeel?

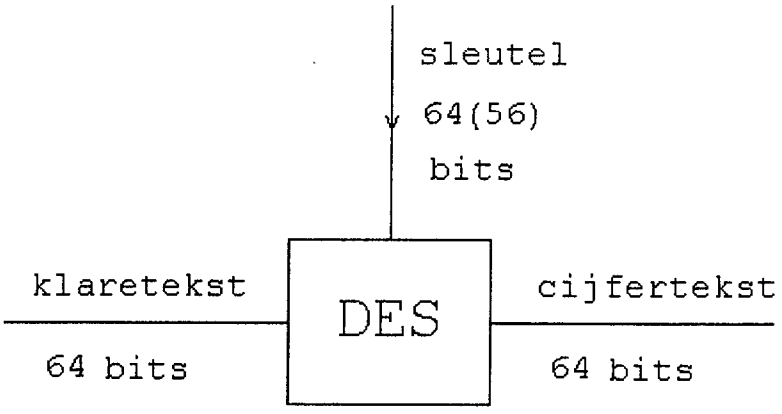
2.5 Moderne cijfers op chips

De cryptosystemen die we tot nu toe hebben bekeken vercijferen de letters uit een tekst één voor één. Een andere manier om teksten te vercijferen is het werken met **Blokcijfers**. Blokcijfers zijn vercijfermethodes die steeds hele groepen tegelijk bewerken. Meestal hebben we het dan over groepen van 64 of 128 bits.

2.5.1 Het algemene principe van een blokcijfer

Blokcijfers worden op chips ingevoerd om hoge snelheden voor de vercijfering en ontcijfering te kunnen halen. De 'tekst' die vercijferd wordt bestaat uit een (mogelijk zeer lange) rij van bits. Normale tekst moet dus van tevoren worden omgezet naar bits. Dit kan door bijvoorbeeld door letters om te zetten naar ASCII code en deze vervolgens te vertalen naar binaire code. Je krijgt dan een lange rij van nullen en enen, de zogenaamde bits.

Het meest gebruikte blokcijfer heet de Data Encryption Standard (DES). DES zit bijvoorbeeld op de Chipper en de Chipknip. DES vercijfert steeds groepjes van 64 bits. In paragraaf 2.5.3. wordt verder uitgelegd hoe dit werkt.



Je doorloopt het proces van links naar rechts om te vercijferen en van rechts naar links om te ontcijferen.

DES heeft ook een sleutel van 64 bits, maar 8 daarvan zijn controle bits om verkeerd ingevoerde bits te kunnen ontdekken. Het aantal verschillende sleutels is dus:

$$2^{56} = 72057594037927936$$

Binnenkort wordt de selectie van de opvolger van DES verwacht. Deze gaat AES (Advanced Encryption Standard) heten. De reden hiervoor is dat DES niet meer als veilig gezien wordt. AES zal waarschijnlijk werken met sleutels van 128, 192 of zelfs 256 bits. Dat maakt het kraken veel moeilijker, want elke extra bit verdubbelt het aantal mogelijke sleutels. Bij 256 loopt het aantal combinaties op tot meer dan een quadriljoen quadriljoen quadriljoen. Dat moet volstaan om voor enkele decennia de vooruitgang van de computertechniek vóór te blijven.

De discussie die rond AES wordt gevoerd kun je volgen op de webpagina van de "Advanced Encryption Standard" http://csrc.nist.gov/encryption/aes/aes_home.htm.

Vraag: Wat is het aantal sleutels van AES bij het tegelijk vercijferen van 128 bits?

2.5.2 Een identiteitscontrole

Gedurende de laatste jaren wordt er steeds meer gebruik gemaakt van verschillende smartcards. Een smartcard is een plastic kaartje ter grootte van een normale bankpas. In plaats van de gewone magneetstrip op je bankkaart, zit er op de smartcard een kleine siliconenchip waarin een grote hoeveelheid informatie kan worden opgeslagen. Smartcards worden veel gebruikt voor:

Telefoonkaarten
De elektronische portomonnaie
Identiteitskaarten
Toegangssleutels
GSM SIMs
Kaarten voor betaald Tv-kijken
Tolkaarten
Klantenkaarten (bij supermarkten etc.)
Enz...

Het voordeel van smartcards is dat de chip op de kaart zelf kan rekenen. Hierdoor is de kaart makkelijker te beveiligen en kunnen vercijferingstechnieken in de kaart worden gebruikt. Bovendien zijn smartcards duurzamer dan de traditionele kaarten met magneetstrips.

Als een smartcard in een kaartlezer wordt gestopt, gaan de kaart en de kaartlezer eerst van elkaar controleren of ze wel door een officiële instantie, zeg de eigen bank, zijn uitgegeven (dus geen vervalsingen zijn). Op elke kaart en in elke kaartlezer zit een kopie van een blokcijfer (dit is nu DES).

Wanneer de bank een kaart maakt voor klant Bob, berekent zij een unieke geheime sleutel k_{Bob} die bij de kaart van Bob hoort en slaat deze op een ontoegankelijke plaats in de chip van de kaart op. De bank gebruikt voor de berekening van k_{Bob} het blokcijfer BC. Dit blokcijfer gebruikt als invoer een uniek identiteitsnummer van Bob, dat we Id_{Bob} noemen. Het blokcijfer BC heeft als sleutel een supergeheime waarde MK (voor meestersleutel, ofwel MasterKey). Het identiteitsnummer Id_{Bob} van Bob is niet geheim. Hierin kunnen naam en rekeningnummer verwerkt zijn. Dus voor k_{Bob} krijg je:

$$k_{Bob} = \text{BC}(\text{MK}, Id_{Bob})$$

De meestersleutel MK is ook aanwezig in de kaartlezer, maar dan extra zwaar beschermd. Als de kaart van Bob in de lezer wordt gestopt, leest de lezer eerst het identiteitsnummer Id_{Bob} uit. De kaartlezer kan nu ook k_{Bob} uitrekenen met:

$$k_{Bob} = \text{BC}(\text{MK}, Id_{Bob})$$

De controle verloopt als volgt:

Controle van de smartcard door de kaartlezer.

De kaartlezer maakt een willekeurig rijtje van 64 nullen en enen. Dit rijtje noemen we even r. De kaartlezer presenteert r als "uitdaging" aan de kaart. De kaart past op r het blokcijfer toe onder zijn geheime sleutel k_{Bob}. Het resultaat hiervan, c, geeft de kaart aan de kaartlezer als zijn "antwoord" op de uitdaging. Dus:

$$c = \mathrm{BC}(k_{Bob}, r)$$

Een andere kaart zal niet in staat zijn het goede antwoord c te geven!

Controle van de kaartlezer door de smartcard.

De kaart maakt nu op zijn beurt een willekeurig rijtje van 64 nullen en enen en presenteert dat als zijn "uitdaging" aan de kaartlezer. Alleen een officieel geïnstalleerde kaartlezer kent MK en kan daarmee met:

$$k_{Bob} = \mathrm{BC}(\mathrm{MK}, Id_{Bob})$$

de sleutel k_{Bob} bepalen uit het identiteitsnummer Id_{Bob}. Met k_{Bob} berekent nu de kaartlezer:

$$c = \mathrm{BC}(k_{Bob}, r)$$

en geeft dat als "antwoord" op de uitdaging aan de kaart.

2.5.3 Iets meer over DES

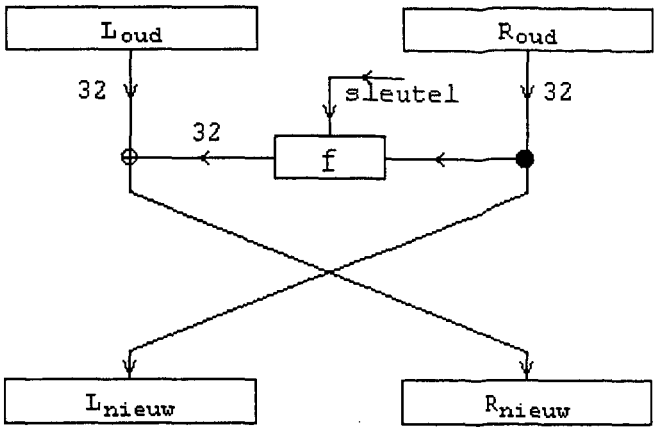
Data Encryption Standard (DES) is een, in 1977 door IBM ontwikkelde, veel gebruikte vercijferingsmethode. Men was er van overtuigd dat deze zo moeilijk te breken was dat de regering van Amerika de uitvoer naar andere landen beperkte, omdat ze bang waren dat het systeem door vijandige regeringen zou worden gebruikt. Tegenwoordig bestaan er gratis versies van de software die ruimschoots te vinden zijn op het Internet.

Bij DES bestaan er zoals je gezien hebt:

$$2^{56} = 72057594037927936$$

mogelijke vercijferringsleutels. Voor elke boodschap wordt de sleutel willekeurig uit dit aantal gekozen. De zender en ontvanger moeten beiden dezelfde geheime sleutel kennen en gebruiken.

DES behandelt ieder binnenkomend groepje van 64 bits door ze in 16 rondes te bewerken. Iedere ronde doet globaal gezien hetzelfde. De 64 bits worden in een linker en een rechterhelft van elk 32 bits verdeeld.



De 32 meest rechtse bits (R_{oud}) worden onveranderd naar links gebracht. Die komen in de volgende ronde aan de beurt. De 32 linker bits (L_{oud}) worden "opgeteld" bij de 32 output bits van een functie f. De eerste output bit van L_{oud} wordt modulo 2 opgeteld (want je wilt nullen en enen houden) bij de eerste output bit van f, de tweede output bit van L_{oud} wordt modulo 2 opgeteld bij de tweede output bit van f, enzovoorts. De f-functie is een vaste functie voor alle rondes. Hiervoor wordt als invoer R_{oud} en een gedeelte van de sleutel gebruikt, om precies te zijn worden er 48 bits van de sleutel gebruikt. De keuze van deze 48 bits verschilt per ronde.

Voor het ontcijferen van DES kan dezelfde chip gebruikt worden als voor het vercijferen. Je kunt alles gewoon in omgekeerde volgorde doorlopen, immers als je in een ronde L_{nieuw} en R_{nieuw} kent, dan ken je ook R_{oud}, want die is gelijk aan L_{nieuw}. Je kunt dan de f-functie uitrekenen, want je kent alle input, en dus kun je ook L_{oud} uitrekenen.

Hoewel dit beschouwd wordt als een "sterke" vercijfering, gebruiken veel bedrijven het zogenaamde "triple DES". Hierbij worden opeenvolgend 3 DES vercijferingen toegepast. Een "sterke" vercijfering wil niet zeggen dat een DES vercijfering niet gebroken kan worden. In 1997 loofde RSA $10.000,- uit voor het breken van een DES vercijferde boodschap. Een gezamenlijke poging op het Internet van ca. 14.000 computergebruikers, die verschillende sleutels probeerden, leverde resultaat na het doorlopen van slechts 18.000.000.000.000.000 van de ca. 72.000.000.000.000.000 sleutels.

Er zullen maar weinig boodschappen die met DES vercijferd zijn op deze manier worden "aangevallen", maar toch.... nog niet zo lang geleden werd een met DES vercijferde boodschap binnen 40 dagen ontcijferd (zie http://news.cnet.com/news/0-1003-200-326872.html?st.ne.fd.mdh). Met het steeds sneller worden van de computers begint men zich toch zorgen te maken over de veiligheid van DES en wordt er gewerkt aan een nieuwe standaard AES (Advanced Encryption Standard).

3 Wiskundige principes

3.1 Modulo rekenen, priemgetallen en grootste gemene delers

In sectie 2.1 heb je al iets kunnen lezen over klokrekenen, oftewel modulo rekenen. Een bekend systeem voor vercijfering, RSA, waarover meer wordt verteld in hoofdstuk 5 maakt veel gebruik van modulo rekenen met priemgetallen. Je kunt daarom in dit hoofdstuk iets lezen over priemgetallen, hoe je die kunt vinden en over het modulo rekenen met priemgetallen.

Een getal groter dan één noem je een priemgetal als je het alleen kunt delen door één en zichzelf. De eerste zes priemgetallen zijn:

2, 3, 5, 7, 11 en 13.*

Met delen bedoelen we dat je een geheel getal overhoudt. We zeggen dat een geheel getal b een deler is van een positief geheel getal a als er een positief geheel getal k bestaat zodanig dat $a = k \cdot b$. Het getal a noem je een veelvoud van b. Als b geen deler is van a dan zeg je dat a niet deelbaar is door b.

Voorbeelden:

3 is een deler van 12 want $12 = 4 \cdot 3$
13 is een deler van 26 want $26 = 2 \cdot 13$
1 is een deler van 13 want $13 = 13 \cdot 1$
13 is een deler van 13 want $13 = 1 \cdot 13$
3 is geen deler van 25 want er bestaat geen geheel getal k waarvoor geldt $25 = k \cdot 3$

Nu geldt volgens de hoofdstelling van de getaltheorie dat elk natuurlijk getal groter dan één is te ontbinden in priemfactoren. Dat wil zeggen dat je elk getal kunt schrijven als het produkt van priemgetallen:

Voorbeelden:

$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$
$21 = 3 \cdot 7$
$3 = 3$
$200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 = 2^3 \cdot 5^2$

Elk priemgetal is dus een deler van oneindig veel positieve getallen groter dan één.

* Je kunt kleine priemgetallen makkelijk vinden met de 'Zeef van Eratostenes' (zie: http://www.utm.edu/research/primes/programs/Eratosthenes/), maar op het internet zijn ook programmaatjes beschikbaar die het n^{de} priemgetal voor je bepalen als je n invoert. (http://www.math.Princeton.EDU/~arbooker/nthprime.html) of kijk eens op http://wims.unice.fr/~wims/wims.cgi?session=NE1116F34F.2&lang=en&module=tool%2Fnumber%2Fprimes.en. Leuke achtergrond informatie over priemgetallen kun je vinden op: http://www.utm.edu/research/primes/largest.html#intro.

Stel eens dat een getal een deler is van twee verschillende getallen, b.v. 3 is een deler van 12 en 3 is ook een deler van 15. Het grootste getal dat zowel een geheel getal a als een geheel getal b deelt noem je de 'grootste gemene deler van a en b'. Dit schrijf je als ggd(a , b).

Voorbeelden:

ggd(11 , 14) = 1
ggd(15 , 42) = 3
ggd(6 , 64) = 2

De grootste gemene deler van meer dan twee getallen is het grootste getal dat deler is van al die getallen.

Voorbeelden:

ggd(6, 8, 10) = 2
ggd(6, 9, 12, 18) = 3
ggd(3 , 4, 5) = 1

Een belangrijke regel bij het berekenen van de ggd is:

Als a en b twee positieve gehele getallen zijn met a > b dan geldt
ggd(a , b) = ggd(a-b, b).

Voorbeelden:

ggd(54, 8) = ggd(46, 8) = ggd(38, 8) = ggd(30, 8) = ggd(22, 8) = ggd(14, 8) = ggd (6,8) = ggd (2, 6) = 2.
ggd(100, 15) = ggd(85, 15) = ggd(70, 15) = ggd (55, 15) = ggd(40, 15) = ggd(25, 15) = ggd(10, 15) = ggd(15, 10) = ggd(5, 10) = 5.

Nu is het natuurlijk niet zo dat je uit deze twee voorbeelden kunt opmaken dat deze regel altijd geldt. Een bewijs dat dit wel zo is gaat als volgt:

Neem aan dat de letters a, b, c, d, k, l, p en q posititieve gehele getallen zijn.
Stel ggd(a , b) = c. Dat betekent dat c een deler is van a en van b. Er bestaan dus getallen k en l zodat geldt: a = k·c en b = l·c. Hieruit volgt dat a - b = k·c - l·c = (k - l)·c en dat betekent dat c een deler is van a - b, dus c is een deler van a - b en van b.

Nu moet je nog bewijzen dat c de grootste deler van b en a - b is. Stel ggd(a - b, b) = d en stel d > c. Hieruit volgt dat d een deler is van b en van a - b. Dus er bestaan getallen p en q zodat geldt: a - b = p·d en b = q·d. Daaruit volgt echter a = p·d + b = p·d + q·d = (p + q)·d dus d is ook een deler van a. En dat kan niet vanwege ggd(a , b) = c. Want dan zou d een grotere deler zijn van a en b, dus moet c wel de grootste deler zijn van b en a – b.

Hoe kun je de grootste gemene deler van twee getallen bepalen? De ggd-berekening in het voorbeeld hierboven kan ook anders. Je kunt zoveel mogelijk keer 8 van 54 in

één keer aftrekken: ggd(54 , 8) = ggd(54 - 6·8 , 8) = ggd(6, 8). Dit noemen we het algoritme van Euclides en het werkt als volgt:

Wat is de ggd van 230 en 64?

$230 = 3 \cdot 64 + 38$
$64 = 1 \cdot 38 + 26$
$38 = 1 \cdot 26 + 12$
$26 = 2 \cdot 12 + 2$
$12 = 6 \cdot 2 + 0$

de ggd(230, 64) = ggd(12,2) = 2.

Dit algoritme levert de volgende 'handige' bijkomstigheid. De ggd van twee getallen is te schrijven als een lineaire combinatie van die twee getallen, dus in het voorbeeld:

$2 = a \cdot 230 + b \cdot 64$,

De getallen a en b zijn makkelijk te vinden met behulp van het algoritme van Euclides dat je net hebt uitgeschreven.

Begin maar eens bij de op één na laatste regel: $\mathbf{26} = 2 \cdot \mathbf{12} + 2$, dus $2 = \mathbf{26} - 2 \cdot \mathbf{12}$, maar in de daarvoor liggende regel kun je ook nog vinden dat $12 = \mathbf{38} - 1 \cdot \mathbf{26}$, dus $2 = 26 - 2 \cdot (38 - 26) = 3 \cdot \mathbf{26} - 2 \cdot \mathbf{38}$ enz. Als je dit uitschrijft krijg je:

$2 = \mathbf{26} - 2 \cdot \mathbf{12} = 26 - 2 \cdot (38 - 26) = 3 \cdot \mathbf{26} - 2 \cdot \mathbf{38} = 3 \cdot (64 - 38) - 2 \cdot (230 - 3 \cdot 64) = 3 \cdot 64 - 3 \cdot (230 - 3 \cdot 64) - 2 \cdot (230 - 3 \cdot 64) = 18 \cdot \mathbf{64} - 5 \cdot \mathbf{230}$

Op het volgende internetsite wordt je de ggd van twee getallen gegeven als je deze invoert en vind je onderaan de pagina de lineaire combinatie van de twee getallen die de ggd oplevert.

http://www.math.sc.edu/~sumner/numbertheory/euclidean/euclidean.html of kijk op: http://wims.unice.fr/~wims/wims.cgi?session=NE1116F34F.2&lang=en&module=tool%2Farithmetic%2Fbezout.en

3.1.1 Opgaven

1. Hoeveel priemgetallen zijn er tussen 1 en 100?
2. a) Bepaal de ggd van 610 en 987. Geef ook de lineaire combinatie.
   b) Bepaal de ggd van 2382 en 237. Geef ook de lineaire combinatie.
3. Bereken de laatste twee cijfers van 1999^{1999} (Hint: probeer het met modulo 100 te berekenen).
4. *Schrijf een programmaatje dat de ggd van twee getallen *m* en *n* uitrekent.
5. *Breid je programmaatje uit zodat het ook de lineaire combinatie van *m* en *n* geeft voor de ggd.

* Deze opgaven zijn pittig. De programmaatjes kunnen zoals aangegeven ook op het internet worden gevonden.

3.2 De Stelling van Fermat

Pierre de Fermat leefde van 1601 – 1665. Hij was advocaat en beoefende wiskunde als hobby. Hij is een van de stichters van de moderne getaltheorie. Veel ontwikkelingen in de getaltheorie zijn het resultaat van pogingen om Fermat's laatste stelling te bewijzen. Deze stelling zegt dat er voor gehele positieve getallen x, y en z, $x^n + y^n = z^n$ geen oplossingen heeft als n >2. Deze stelling is pas in 1994 bewezen door de Britse wiskundige Andrew Wiles.

Een andere stelling van Fermat, ook wel de kleine stelling van Fermat genoemd is:

De kleine stelling van Fermat
Als *p* een priemgetal is en *a* een getal dat niet door *p* deelbaar is, dan geldt

$$a^{p-1} \equiv 1 \pmod{p}.$$

Voorbeelden:

a = 2,
p = 5,

$a^{p-1} = 2^4 = 16 \equiv 1 \pmod 5$

a = 10
p = 7

$10^{p-1} = 10^6 = 1.000.000 = 142857 \cdot 7 + 1 \equiv 1 \pmod 7$

3.2.1 Bewijs van de kleine stelling van Fermat

Bij het bewijs van de stelling van Fermat maak je gebruik van de volgende hulpstelling:

Hulpstelling
Als *p* een priemgetal is en *a* een getal dat niet door *p* deelbaar is, dan geldt als $a \cdot i \equiv a \cdot j \pmod p$, dan $i \equiv j \pmod p$.

Voorbeeld:
p = 7,
a = 3,

Als je de getallen van {0, 1, 2, 3, 4, 5 ,6} met 3 vermenigvuldigt modulo 7 dan krijg je weer de getallen {0, 1, 2, 3, 4, 5, 6}, maar dan in een andere volgorde. Je kunt dus alleen maar $3 \cdot i \equiv 3 \cdot j \pmod 7$ krijgen als $i \equiv j \pmod 7$.

Bewijs van de hulpstelling
Als je zegt dat $a \cdot i \equiv a \cdot j \pmod{p}$ dan zeg je eigenlijk dat $a \cdot i$ en $a \cdot j$ een p-voud verschillen. Met andere woorden p is een deler van $a \cdot i - a \cdot j$, dus p is een deler van $a(i - j)$. Maar p is priem en a is niet deelbaar door p. Dus geldt dat p een deler is van $i - j$, oftewel i is een aantal keren p rest j en dat schrijven we als $i \equiv j \pmod{p}$.

Laten we nu nog eens kijken naar het voorbeeld in de hulpstelling. Kijk naar de getallen {1, 2, 3, 4, 5, 6} (de 0 ontbreekt) en vermenigvuldig ze allemaal met a, dus met 3.

$3 \cdot \{1, 2, 3, 4, 5, 6\} = \{3, 6, 9, 12, 15, 18\}$

Neem de laatste getallen modulo p, (dus 7), dan krijg je: {3, 6, 2, 5, 1, 4}. Dit is weer het originele rijtje, alleen in een andere volgorde. Als twee rijtjes hetzelfde zijn, dan moeten ook de producten van de getallen in die rijtjes hetzelfde zijn, dus:

$(3x1)x(3x2)x(3x3)x(3x4)x(3x5)x(3x6) \equiv 1x2x3x4x5x6 \pmod 7$, dit is hetzelfde als:
$3x3x3x3x3x3x1x2x3x4x5x6 \equiv 1x2x3x4x5x6 \pmod 7$, ofwel
$3^6x1x2x3x4x5x6 \equiv 1x2x3x4x5x6 \pmod 7$.

Als je nu dezelfde factoren wegstreept, dan krijg je:

$3^6 \equiv 1 \pmod 7$, dus $a^{p-1} \equiv 1 \pmod p$ en dat is de stelling van Fermat.

3.3 De Stelling van Euler

Leonhard Euler leefde van 1707 – 1783. Hij was een Zwitsers wiskundige en een pupil van Johann Bernoulli. In 1727 was hij een lid van de Universiteit van St. Petersburg op invitatie van Catherine I, keizerin van Rusland. In 1741 werd hij professor in de wiskunde aan de Berlijnse Universiteit op aandringen van de Pruisische koning Frederik de Grote. Euler keerde in 1766 terug naar St. Petersburg en bleef daar tot zijn dood in 1783. Hoewel hij sinds zijn 30ste vrijwel blind was, produceerde hij een aantal zeer belangrijke wiskundige werken en honderden wiskundige en wetenschappelijke memoires.

De stelling van Euler die je hier gebruikt gaat nog een stapje verder dan de stelling van Fermat. Eerst definiëren we de Euler functie ϕ.

Definitie
De functie ϕ van Euler telt voor elk natuurlijk getal m hoeveel kleinere positieve getallen er zijn die geen factor met m gemeen hebben.

$\phi(m)$ = aantal getallen $1 \leq i < m$ met ggd(i, m) = 1.

Voorbeelden:

- m = 7. De getallen 1, 2, 3, 4, 5 en 6 zijn kleiner dan 7 en hebben geen factor met 7 gemeen. Dus $\phi(7) = 6$.
- m = 10. De getallen 1, 3, 7 en 9 zijn kleiner dan 10 en hebben geen factor met 10 gemeen. Dus $\phi(10) = 4$.

Het is natuurlijk duidelijk dat $\phi(p) = p - 1$ als p een priemgetal is. Al de getallen 1, 2, …, p – 1 zijn kleiner dan p en hebben er geen factor mee gemeen. Voor het product van twee priemgetallen is het echter wat moeilijker om de ϕ te bepalen.

Voorbeeld:

m = 10, nogmaals.

mogelijke getallen	1	2	3	4	5	6	7	8	9	10
weg					5					10
weg		2		4		6		8		10
dubbel weg										10
over	1		3				7		9	

Hier geldt $\phi(10) = 10 - 2 - 5 + 1 = 4$
(dit is hetzelfde als (5 - 1)(2 – 1))

Algemeen gezegd: Als p en q verschillende priemgetallen zijn, geldt dat

$\phi(p \times q) = p \times q - p - q + 1 = (p - 1)(q - 1)$ (ofwel $\phi(p)\cdot\phi(q)$ als p en q niet gelijk zijn),

immers, van de $p \times q$ getallen met $1 \leq i \leq p \times q$ zijn er p getallen die door q deelbaar zijn (alle veelvouden van p) en q getallen die door p deelbaar zijn (alle veelvouden van q). Deze $p + q$ mogelijkheden moet je dus wegschrappen. Er is echter één getal zowel door p als door q deelbaar en dat heb je net twee keer weggeschrapt. Je moet er dus weer 1 mogelijkheid bij optellen.

De meeste getallen kun je echter niet als een vermenigvuldiging van slechts twee verschillende priemgetallen schrijven. Je kunt wel elk bestaand geheel getal als het product van meerdere priemgetallen schrijven, bijvoorbeeld: $21000 = 2^3 \times 3 \times 5^3 \times 7$. Is hier nu ook makkelijk de ϕ van te bepalen? Wat gebeurt er als p en q gelijk zijn?

Formule van Euler voor $\phi(n)$

Voor een getal $n = p^a q^b r^c s^d$*, (p, q, r en s, zijn priemgetallen en a, b, c, en d zijn gehele getallen groter of gelijk aan 1) geldt dat:

$$\phi(n) = p^{a-1} q^{b-1} r^{c-1} s^{d-1} \cdot (p - 1)(q - 1)(r - 1)(s - 1)$$

Hoe kom je hieraan? We kijken eerst eens naar een 'simpel' geval $n = p^a$.

* Je kijkt hier naar een voorbeeld met 4 priemgetallen, maar het kunnen er ook meer of minder zijn.

p is een priemfactor van n. De getallen die kleiner zijn dan n en een factor met n gelijk hebben zijn dan: p, $2p$, $3p$, $4p$, ..., $p^{a-1} \cdot p$. Dit zijn er p^{a-1}. Er zijn dus $n - p^{a-1}$ getallen die géén factor met n gemeen hebben en dit is hetzelfde als $p^a - p^{a-1} = p^{a-1}(p-1)$. Met andere woorden $\phi(n) = p^{a-1}(p-1)$. Je had al gezien dat $\phi(p \times q) = p \times q - p - q + 1 = (p-1)(q-1)$ (ofwel $\phi(p) \cdot \phi(q)$ als p en q niet gelijk zijn).

Met de Chinese Reststelling* is te bewijzen dat ook $\phi(u \cdot v \cdot w \cdot x) = \phi(u)\phi(v)\phi(w)\phi(x)$, met $u = p^a$, $v = q^b$, $w = r^c$ en $x = s^d$ en u, v, w, en x zijn onderling priem.**
Dan volgt dat:

$$\phi(n) = \phi(p^a)\phi(q^b)\phi(r^c)\phi(s^d) = p^{a-1} q^{b-1} r^{c-1} s^{d-1} \cdot (p-1)(q-1)(r-1)(s-1).$$

Dan nu de stelling van Euler.

Stelling van Euler

Als a geen factor gemeen heeft met m dan geldt dat $a^{\phi(m)} \equiv 1 \pmod{m}$.

Voorbeeld:

Als je het laatste cijfer van 1997^{1997} wilt uitrekenen, zoek je eigenlijk het antwoord op $1997^{1997} \pmod{10}$. Je wilt dus het laatste cijfer in 7^{1997} weten, want $1997 \equiv 7 \pmod{10}$. Verder is $1997 = 499 \times \phi(10) + 1$, dus kun je vanwege de stelling van Fermat schrijven:

$$7^{1997} \equiv 7^{499 \times \phi(10) + 1} \equiv 7^{499 \times 4} \times 7 \equiv (7^4)^{499} \times 7 \equiv 1^{499} \times 7 \equiv 7 \pmod{10}.$$

Bewijs van de Stelling van Euler.
Het bewijs van de Stelling van Euler verloopt precies hetzelfde als het bewijs van de Stelling van Fermat.

Het bewijs bestaat dus uit de volgende stappen.

1) **Maak een lijst van alle getallen tussen 1 en m die geen factor gemeen hebben met m (er zijn er $\phi(m)$). Dit is lijst A.**
2) **Vermenigvuldig al de getallen in lijst A met a. Dit geeft lijst B.**
3) **Observeer dat modulo m lijst B op de volgorde na hetzelfde is als lijst A.**
4) **Modulo m is dus het product van alle elementen in de eerste lijst gelijk aan dat van de tweede lijst.**
5) **Deel aan beide kanten dezelfde factoren weg.**
6) **Schrijf op wat je overhoudt. Dat is precies wat bewezen moest worden.**

* http://www.cut-the-knot.com/blue/chinese.html

** Onderling priem wil zeggen dat ggd$(u,v,w,x) = 1$.

3.3.1 Opgaven

1. Hoe groot zijn $\phi(15)$ en $\phi(35)$?
2. * Schrijf een programmaatje dat de ϕ van een gegeven getal m uitrekent, voor $m < 10000$.
3. ** Controleer het voorbeeld waarin je het laatste getal van 1997^{1997} uitrekent met de programmaatjes die je in 3.1.1 en 3.3.1 hebt gemaakt.
4. Controleer de Stelling van Euler voor het geval dat $m = 15$ en $a = 4$ op de manier zoals in het bewijs hierboven is uitgelegd. (Bewijs dus dat $4^8 \equiv 1 \pmod{15}$).
5. Bereken $123^{123} \pmod{15}$.
6. Probeer als in het voorbeeld met m = 10, met behulp van een tabel $\phi(30)$ te berekenen. Controleer je antwoord met de formule van Euler.
7. Bereken:
   a) $\phi(126)$
   b) $\phi(1265)$
   c) $\phi(215689)$
   d) $\phi(369879)$
8. Laat zien dat: $\phi(n) = n \cdot (1 - 1/p)(1 - 1/q)(1 - 1/r)(1 - 1/s)$ als $n = p^a q^b r^c s^d$

3.4 Machtsverheffen, worteltrekken en logaritmes nemen

In de vorige paragraaf heb je al kunnen zien dat als je het laatste getal van een macht zoekt of de laatste twee getallen, je dit op een vrij simpele manier met modulorekenen kunt oplossen. Bestaat er nu ook zoiets voor machtsverheffen? Hoe gaat dat modulo een groot getal? Wat doe je bijvoorbeeld als je $6^{4371} \pmod{99991}$ moet uitrekenen? Je berekent in ieder geval niet eerst 6^{4371} (dit is heel groot) om daarna het antwoord modulo 99991 te reduceren. Een beter idee is alle deelberekeningen klein te houden door elke tussenresultaat meteen modulo 99991 te reduceren. Maar aan welke deelberekeningen denk je dan?

Voor machten bestaan een aantal regels waar je handig gebruik van kunt maken.

Regel 1: Bij de vermenigvuldiging van een macht met een andere macht die beide hetzelfde grondtal hebben, mag je de exponenten bij elkaar optellen, dus $a^x \cdot a^y = a^{x+y}$.

Regel 2: Bij het verheffen van een macht tot een macht mag je de exponenten met elkaar vermenigvuldigen, dus $(a^x)^y = a^{x \cdot y}$.

Het getal 4371 is net als elk ander getal ook binair te schrijven, nl. 1000100010011. Dit betekent dat $4371 = 2^{12} + 2^8 + 2^4 + 2 + 1$. (De plaatsing van de enen correspondeert met de exponenten.)

Dit is hetzelfde als $4371 = 4096 + 256 + 16 + 2 + 1$. Met Regel 1 kun je dus schrijven:

$$6^{4371} = 6^{4096 + 256 + 16 + 2 + 1}$$

en met Regel 2 wordt dat:

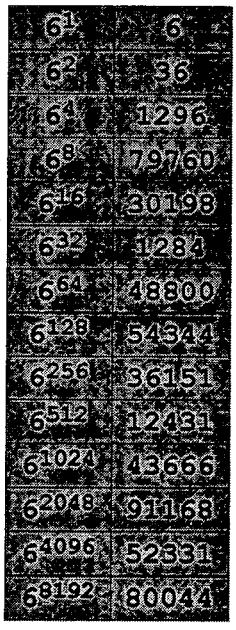
---

* Deze opgave is vrij pittig.
** Indien de desbetreffende opgaven gemaakt zijn.

$6^{4371} = 6^{(2^{12})} \cdot 6^{(2^8)} \cdot 6^{(2^4)} \cdot 6^{(2^1)} \cdot 6 \cdot$

Je berekent 6^2 (mod 99991), 6^4 (mod 99991), 6^8 (mod 99991) enz. door steeds het voorgaande antwoord te kwadrateren en dan de uitkomst te reduceren modulo 99991.

Uit dit lijstje pak je nu de benodigde machten: $6^{(2^{12})}$, $6^{(2^8)}$, $6^{(2^4)}$, $6^{(2^1)}$ en 6 en vermenigvuldigd deze met elkaar modulo 99991.



$6^{(2^{12})} \cdot 6^{(2^8)} \cdot 6^{(2^4)} \cdot 6^{(2^1)} \cdot 6$ (mod 99991) is dus gelijk aan:

$$52331 \bullet 36151 \bullet 30198 \bullet 36 \bullet 6 \equiv 24455 \text{ (mod 99991)}$$

Opmerking:

Nog iets over modulorekenen

Veel vercijferingsmethoden maken gebruik van modulorekenen. In het voorbeeld met *cleopatra* kreeg je voor *c*: $c + 7 = 2 + 7 = 9 = j$. Nu wil de onderschepper van een stuk tekst natuurlijk graag de oplossing weten van $x_i \equiv 9$ (mod 26), x_i zijn alle letters in de tekst (hier *cleopatra*[*]) en in dit geval is dat met "Exhaustive key search" niet al te moeilijk. Maar wat gebeurt er als een tekst is omgezet in getallen? Is het oplossen van $x_i \equiv 9$ (mod 26) dan nog zo simpel? Het probleem is dat je niet weet hoeveel keer 26 van x_i is afgetrokken. Je kunt hier dus alleen maar mogelijke oplossingen geven. Deze hebben dan de vorm $x_i = 26 \cdot t + 9$, waarin t een geheel getal is. Problemen van de vorm $9 \cdot x_i \equiv 4$ (mod 26) zijn nog iets ingewikkelder. We behandelen hiervan een voorbeeld.

[*] Dus $x_1 = c$, $x_2 = l$, $x_3 = e$, *enz.*

Voorbeeld:

- $10 \cdot s \equiv 2 \pmod 7$

  nu kijk je naar ggd(10,7) = 1 en je kijkt naar de lineaire combinatie van 10 en 7 die de ggd oplevert: $3 \cdot 7 - 2 \cdot 10 = 1$. Als je nu modulo 7 rekent, dan krijg je dat $-2 \cdot 10 \equiv 1 \pmod 7$ en $-4 \cdot 10 \equiv 2 \pmod 7$, dus $-4 \equiv 2/10 \pmod 7$.
  Met andere woorden:
  $s \equiv -4 \pmod 7 \equiv 3 \pmod 7$.
  De oplossing voor s is nu: $s = 7 \cdot t + 3$, met t een geheel getal.

Het tegenovergestelde van machtsverheffen voor grote moduli is, zelfs met de snelste computers, ondoenlijk.

Voor een opgave zoals "bepaal m zodat $m^{4371} \equiv 34455 \pmod{99991}$", ofwel $m \equiv \sqrt[4371]{34455} \pmod{99991}$, (Je hebt het dan over de 4371^{ste} wortel van 34455.) kun je niet veel meer doen dan $m = 1,2,3, \ldots$ uitproberen totdat je 34455 tegenkomt. Hiervan wordt gebruik gemaakt in het RSA cryptosysteem, dat in hoofdstuk 5 wordt behandeld.

Voor een probleem als "bepaal e zodat $6^e \equiv 34455 \pmod{99991}$", ofwel $e \equiv {}^6\log 34455$ is er ook niet veel beter dan $e = 1, 2, 3, \ldots$ uit te proberen. Hiervan wordt gebruik gemaakt in het Diffie-Hellman cryptosysteem,

http://www.apocalypse.org/pub/u/seven/diffie.html,
http://www.dstc.qut.edu.au/javaus/demo/about.html,
http://www.ece.orst.edu/~rodrigfr/ECE573/project/.

3.4.1 Opgaven

1. Geef de binaire uitdrukking voor:
   a) 13254
   b) 2586
   c) 65899
2. *Lees http://www.cut-the-knot.com/blue/chinese.html en probeer daarna de oplossingen van de volgende stelsels vergelijkingen te bepalen:
   a) $x \equiv 1 \pmod 2$
      $x \equiv 2 \pmod 5$
      $x \equiv 2 \pmod 7$
   b) $t \equiv 1 \pmod 2$
      $t \equiv 0 \pmod 3$
      $t \equiv 5 \pmod{10}$
3. Bereken:
   a) $5^{1033} \pmod{1997}$
   b) $6^{4014} \pmod{525}$

* Deze opgave kan desgewenst worden overgeslagen.

4 Cryptosystemen met openbare sleutels; het grondidee

Sinds er computernetwerken bestaan komt het vaak voor dat twee personen onderling via een netwerk communiceren en dat zij hun communicatie willen beschermen zonder dat ze van tevoren een gemeenschappelijk sleutel hebben afgesproken. Vaak kennen ze elkaar niet eens. Denk bijvoorbeeld aan een bedrijf dat je op het web gevonden hebt en waar je wat van wilt gaan bestellen en betalen met je VISA-kaart. Je wilt natuurlijk niet dat iedereen weet wat jouw VISA-kaartnummer is. Nog vaker is het zo dat de ontvanger van jouw boodschap ook absolute zekerheid wil hebben dat de boodschap werkelijk van jou komt. Bovendien wil het bedrijf (en jijzelf) de absolute zekerheid dat er niet met de boodschap geknoeid is door anderen. Dit is niet op te lossen met de symmetrische systemen van hoofdstuk 2.

In 1976 bedachten de Amerikanen Diffie en Hellman een oplossing:

Iedere gebruiker van het communicatienet maakt twee rekenmethodes (algoritmen) die op een bepaalde manier bij elkaar moeten horen (je zult verderop zien hoe). Een persoon *P* maakt dus:

- een openbaar algoritme OpenbaarAlgP,
- een geheim algoritme GeheimAlgP.

(OpenbaarAlgP en GeheimAlgP zijn een soort functies, dus om een vergelijking te maken, je schrijft OpenbaarAlgP(x) net als je f(x) zou schrijven.)
Het GeheimAlgP mag je niet uit het OpenbaarAlgP kunnen halen omdat OpenbaarAlgP bekend wordt gemaakt, b.v. op een webpagina of op briefpapier. Persoon *P* is zelf verantwoordelijk voor het geheim houden van het algoritme GeheimAlgP.

4.1 Geheimhouding

Stel er is een persoon, Alice, die een boodschap heeft voor een andere persoon, Bob. Andere personen, die misschien het verstuurde bericht onderscheppen, mogen niet achter de echte boodschap komen. Alice zoekt het openbare algoritme OpenbaarAlgBob van Bob op en past dat toe op m . Alice zendt dan:

$$c = \text{OpenbaarAlgBob}(m).$$

Bob gebruikt GeheimAlgBob, dat hij alleen kent, om m uit c te berekenen:

$$\text{GeheimAlgBob}(c) = m.$$

Je ziet nu gelijk aan welke relatie de twee algoritmes OpenbaarAlgBob en GeheimAlgBob moeten voldoen: als je op m eerst OpenbaarAlgBob loslaat en daarna GeheimAlgBob op de uitkomst daarvan moet er weer m uitkomen. Dus:

$$\text{OpenbaarAlgBob}(\text{GeheimAlgBob}(m)) = m,$$

en dit moet gelden voor alle mogelijke boodschappen m. Bovendien moet deze relatie voor de algoritmes van elke gebruiker gelden.

Denk bijvoorbeeld voor OpenbaarAlgBob aan een dik woordenboek Nederlands-Swahili en voor GeheimAlgBob aan het corresponderende woordenboek Swahili-Nederlands. Deze vergelijking klopt misschien niet helemaal, maar zonder het woordenboek Swahili-Nederlands is het eigenlijk vrijwel ondoenlijk om een woord in het Swahili terug te vertalen naar het Nederlands.

4.2 Een digitale handtekening

Stel Alice is niet geïnteresseerd in geheimhouding, maar wil wel haar boodschap m van een handtekening voorzien om Bob er zeker van te laten zijn dat de boodschap van haar komt. Ze past dan haar eigen geheime algoritme GeheimAlgAlice op m toe en stuurt:

$$c = \text{GeheimAlgAlice}(m).$$

Bob zoekt het openbare algoritme OpenbaarAlgAlice van Alice op en past het toe op c om m te krijgen.

$$\text{OpenbaarAlgAlice}(c) = m.$$

dus als je GeheimAlgAlice op m loslaat en vervolgens OpenbaarAlgAlice op de uitkomst daarvan moet hier weer m uitkomen, en ook dit moet gelden voor alle mogelijke boodschappen m en voor de algoritmes van elke gebruiker, dus:

$$\text{OpenbaarAlgAlice}(\text{GeheimAlgAlice}(m)) = m.$$

Het idee hierachter is dat alleen Alice met de goede c op de proppen kan komen omdat alleen zij GeheimAlgAlice kent.

4.3 Beide: geheimhouding en handtekening

Nu moeten de relaties die je in 4.1 en 4.2 hebt gezien allebei gelden, dus:

$$\text{OpenbaarAlgBob}(\text{GeheimAlgBob}(m)) = m \text{ en}$$
$$\text{OpenbaarAlgAlice}(\text{GeheimAlgAlice}(m)) = m.$$

Alice zendt:

$$c = \text{OpenbaarAlgBob}(\text{GeheimAlgAlice}(m)).$$

Bob berekent:

$$\text{OpenbaarAlgAlice}(\text{GeheimAlgBob}(c))$$
$$=$$
$$\text{OpenbaarAlgAlice}(\text{GeheimAlgBob}(\text{OpenbaarAlgBob}(\text{GeheimAlgAlice}(m))))$$
$$=$$

OpenbaarAlgAlice(GeheimAlgAlice(m))

=

m

en hij bewaart als bewijs dat de boodschap m werkelijk van Alice komt GeheimAlgBob(c), omdat immers geldt:

GeheimAlgBob(c)

=

GeheimAlgBob(OpenbaarAlgBob(GeheimAlgAlice(m)))

=

GeheimAlgAlice(m)

en dat is de handtekening van Alice over m.

5 Het RSA systeem

5.1 Het systeem

De principes van de openbare sleutels die in hoofdstuk 4 staan beschreven zijn erg algemeen. Een systeem dat op deze manier werkt is het RSA systeem. Het RSA systeem werd in 1978 door R.L. Rivest, A. Shamir en L. Adleman uitgevonden. (Heel soms kom je ook wel de naam MIT systeem tegen.) Dit systeem maakt gebruik van de stelling van Euler. (zie hoofdstuk 3).

5.1.1 Voorbereidingen

Om het RSA systeem te kunnen toepassen moet elke deelnemer een aantal voorbereidingen uitvoeren. Hieronder zie je wat één deelnemer, Bob, doet.

Stap 1: Keuze van de priemgetallen

Bob kiest twee verschillende priemgetallen en hij noemt ze p_B en q_B. (De andere deelnemers aan het systeem moeten hun eigen priemgetallen kiezen.) Hij heeft bijvoorbeeld gebruik gemaakt van een programmaatje zoals je dat vindt op: http://www.math.Princeton.EDU/~arbooker/nthprime.html. Stel dat Bob heeft gekozen voor:

99989 en 99991

Verder rekent Bob ook het produkt van deze twee getallen uit en noemt dat n_B, dus $n_B = p_B \cdot q_B$.

$n_B = 9998000099$

Stap 2: Keuze van de vercijferingsexponent

Bob kiest een willekeurige vercijferingsexponent uit en noemt die e_B. Deze e_B mag geen factor gemeen hebben met $\phi(n_B) = (p_B - 1)(q_B - 1)$. Vanwege de stelling van Euler geldt dan dat $e_B^{\phi(\phi(n_B))} \equiv 1 \pmod{\phi(n_B)}$.

De willekeurige e_B die Bob hier heeft gekozen is: 11111357.
Hij heeft dus nu:

$p_B = 99989$
$q_B = 99991$
$n_B = 9998000099$
$\phi(n_B) = (p_B - 1)(q_B - 1) = 99988 \cdot 99990 = 9997800120$
$e_B = 11111357$
$\text{ggd}(e_B, \phi(n_B)) = 1$

Stap 3: Keuze van de ontcijferingsexponent

Nu berekent Bob een bijbehorende ontcijferingsexponenent d_B (d = decryptie), waarvoor geldt dat:

$$e_B \cdot d_B \equiv 1 \pmod{\phi(n_B)}.$$

Deze is vrij makkelijk te bepalen, want we weten al dat $e_B^{\phi(\phi(n_B))} \equiv 1 \pmod{\phi(n_B)}$. Dit is hetzelfde als $e_B \cdot e_B^{\phi(\phi(n_B)) - 1} \equiv 1 \pmod{\phi(n_B)}$, dus $d_B = e_B^{\phi(\phi(n_B)) - 1}$.

In het voorbeeld van Bob is $d_B = 11111357^{\phi(9997800120) - 1} \pmod{9997800120}$.

In paragraaf 3.3 heb je gezien hoe je $\phi(9997800120)$ moet bepalen, nl. $\phi(9997800120) = \phi(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 101 \cdot 3571) = 2^2 \cdot 3^1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 100 \cdot 3570 = 2056320000$, dus $d_B = 11111357^{2056320000 - 1} \pmod{9997800120}$.

Overigens kun je de factorisatie van een getal in priemfactoren laten berekenen op: http://wims.unice.fr/~wims/wims.cgi. (N.B. er wordt geen beperking gesteld aan de lengte van het getal, wel aan de rekentijd, dit is maximaal 20 seconden)

Met de stelling van Euler geldt bovendien dat $11111357^{2056320000} \equiv 1 \pmod{9997800120}$ en dus $11111357 \cdot 11111357^{2056320000 - 1} \equiv 1 \pmod{9997800120}$.

Om d_B te berekenen kun je gebruik maken van de methode die je hebt gezien in paragraaf 3.4:

$$d_B = 42643373.$$

Maar het kan ook anders. Bij het berekenen van de ggd van twee getallen heb je gezien dat je met behulp van het algoritme van Euclides je die twee getallen kunt schrijven als een lineaire combinatie die de ggd oplevert. Je weet dat:

$$\text{ggd}(e_B, \phi(n_B)) = 1$$

dus kun je schrijven $a \cdot e_B + b \cdot \phi(n_B) = 1$. Als je dit nu modulo $\phi(n_B)$ berekent, dan krijg je dat $a \cdot e_B + 0 = 1 \pmod{\phi(n_B)}$, dus $d_B = a$. Met andere woorden alles wat je hoeft te doen is het algoritme van Euclides toe te passen op e_B en $\phi(n_B)$. Hiervoor kun je gebruik maken van het applet dat je vindt op:
http://www.math.sc.edu/~sumner/numbertheory/euclidean/euclidean.html
of van het programmaatje dat je zelf hebt gemaakt in opgave 4 en 5 van paragraaf 3.1.1.

Stap 4: Bekendmaking van *n* en *e*.
Bob maakt nu: $n_B = 9998000099$ en $e_B = 11111357$ algemeen bekend, maar houdt $d_B = 42643373$ en de priemgetallen $p_B = 99989$ en $q_B = 99991$ geheim.

(Onthoud dat alle andere deelnemers dit ook met hun eigen n, e, d, p en q hebben gedaan.)

5.1.2 RSA voor geheimhouding

Vercijfering
In paragraaf 4.1 heb je gezien hoe Alice een vercijferde boodschap naar Bob verstuurde door het openbare algoritme van Bob op haar boodschap los te laten. Hieronder staat een voorbeeld van een boodschap waarop de getallen die Bob in 5.1.1 heeft voorbereid zijn toegepast.

Stel Alice wil het getal 1122334455 versturen. (In werkelijkheid zal een boodschap bestaan uit letters die eerst vertaald moeten worden in een getal, door bijvoorbeeld gebruik te maken van de ASCII-code. Het getal moet wel kleiner zijn dan n_B, want je rekent modulo n_B.)

Alice zoekt de openbare waarden van Bob op: $n_B = 9998000099$ en $e_B = 11111357$. Ze berekent nu:

$$1122334455^{11111357} \pmod{9998000099} = 4935662754$$

(Het algoritme van Bob is een soort functie, eigenlijk kun je lezen:
$\text{OpenbaarAlgBob}(m) = m^{11111357} \pmod{9998000099} = 4935662754$)

Afluisteraar
Eva is een afluisteraar en zij onderschept de vercijferde boodschap van Alice. De waarden $n_B = 9998000099$ en $e_B = 11111357$ zijn openbaar, dus die kent zij ook en ze weet dus dat

$$\text{Boodschap}^{11111357} = 4935662754 \pmod{9998000099}$$

Ze kan niet veel anders doen dan voor de boodschap 1, 2, 3, …, 9998000098 uit te proberen. Dit is niet leuk en zeker ondoenlijk als n_B en de boodschap getallen van 200 tot 500 cijfers lang zijn.

Ontcijfering door Bob
Bob is de enige die de geheime oncijferingsexponent $d_B = 42643373$ kent en kan dus uitrekenen:

$4935662754^{42643373} \pmod{9998000099} \equiv 1122334455$ en dit is de originele boodschap.

Waarom klopt dit nu? Nou zeg eens dat de boodschap 1122334455 gelijk is aan m en dat de vercijferde boodschap 4935662754 gelijk is aan c. Dan geldt:

$$c^{d_B} \overset{\text{vercijferingsregel}}{\equiv} (m^{e_B})^{d_B} \overset{\text{def van } d_B}{\equiv} m^{e_B d_B} \equiv m^{1+x\cdot\phi(n_B)} \overset{\text{Euler}}{\equiv} m \cdot m^{\phi(n_B)x} \equiv m \cdot 1 \equiv m \pmod{n_B}$$

5.1.3 Een "echt" voorbeeld

Vercijfering
Je gaat een stuk tekst vercijferen dat je gecodeerd naar je vriend wilt sturen, die $p = 13$ en $q = 23$ heeft gekozen. Zijn n is dus: 13 x 23 = 299. Als e neemt hij 5.

Stel dat je de volgende tekst wil versturen:

" Stuur 30% van jouw saldo naar mijn rekening nu!"

Je kunt dit natuurlijk niet op deze manier zomaar vercijferen. Eerst zet je de tekst om in getallen. Daar kun je zelf iets voor verzinnen, maar je vriend moet dan ook wel weten wat je gedaan hebt. Normaal gesproken zet je zo'n tekst om in ASCII-code. Dit kun je handmatig doen, (de codes vind je op: http://www.mindspring.com/~jc1/serial/Resources/ASCII.html) maar je kunt hiervoor ook een programmaatje gebruiken dat je bijvoorbeeld zelf hebt gemaakt of die je kunt vinden op: http://www.breezin.net/Software/software.html#EasyASCII

De code van jouw tekst is:

{83, 116, 117, 117, 114, 32, 51, 48, 37, 32, 118, 97, 110, 32, 106, 111, 117, 119, 32, 115, 97, 108, 100, 111, 32, 110, 97, 97, 114, 32, 109, 105, 106, 110, 32, 114, 101, 107, 101, 110, 105, 110, 103, 32, 110, 117, 33}

Je vercijfert de tekst door elk getal apart tot de macht $e = 5$ te verheffen en dat reduceren modulo $n = 299$, dit levert:

{291, 116, 78, 78, 160, 54, 181, 55, 176, 54, 105, 158, 210, 54, 84, 11, 78, 58, 54, 46, 158, 75, 16, 11, 54, 210, 158, 158, 160, 54, 44, 27, 84, 210, 54, 160, 238, 191, 238, 210, 27, 210, 51, 54, 210, 78, 180}

Ontcijfering door je vriend
Je vriend wil weten wat je hebt geschreven. Zijn geheime d berekent hij als volgt:

$\phi(299) = \phi(13 \times 23) = 13^0 \times 23^0 \times 12 \times 22 = 264$
$1 = 53 \cdot 5 - 1 \cdot 264$
$e \cdot d \equiv 1 \pmod{264}$, dus $d = 53$

Je vriend verheft elk getal in jouw vercijferde code tot de macht 53 en reduceert het antwoord modulo 299. Hij krijgt dan

{83, 116, 117, 117, 114, 32, 51, 48, 37, 32, 118, 97, 110, 32, 106, 111, 117, 119, 32, 115, 97, 108, 100, 111, 32, 110, 97, 97, 114, 32, 109, 105, 106, 110, 32, 114, 101, 107, 101, 110, 105, 110, 103, 32, 110, 117, 33}

en hij converteert vervolgens deze getallen weer terug van ASCII code naar gewone symbolen:

Stuur 30% van jouw saldo naar mijn rekening nu!

5.1.4 RSA voor het zetten van een handtekening

Alice heeft haar eigen RSA getallen gekozen.
$p_A = 99761$,
$q_A = 100151$ en
$e_A = 123454321$.

Dit levert:
$n_A = 99761 \times 100151 = 9991163911$,
$\phi(n_A) = 99760 \times 100150 = 9990964000$ en
$d_A = 24888081$.

Alice wil de boodschap 111222333 versturen naar Bob voorzien van een handtekening. Ze is niet geinteresseerd in geheimhouding van haar boodschap. Alice gebruikt haar geheime exponent $d_A = 24888081$ en berekent:

$111222333^{24888081} \pmod{9991163911} \equiv 9587290538$ en stuurt dit als cijfertekst naar Bob.

Controleren van de handtekening
Bob ontvangt de cijfertekst 9587290538 waarvan beweert wordt dat die van Alice komt. Hij zoekt de openbare algoritmes $n_A = 9991163911$ en $e_A = 123454321$ van Alice op en berekent:

$9587290538^{123454321} \pmod{9991163911} \equiv 111222333$.

Alleen Alice kan 111222333 tot 9587290538 converteren, omdat zij de enige is die d_A kent en alleen het getal 9587290538 heeft de bijzondere eigenschap dat de openbare algoritmes $n_A = 9991163911$ en $e_A = 123454321$ van Alice het terugvoeren naar 111222333. Iedereen kan dus de boodschap van Alice vinden en de handtekening controleren.

5.1.5 RSA voor geheimhouding en handtekening

Als Alice niet wil dat iedereen de boodschap kan vinden, moet ze eerst een handtekening zetten over haar boodschap m en dan het resultaat voor Bob vercijferen.

$$c \equiv (m^{d_A} \pmod{n_A})^{e_B} \pmod{n_B}$$

Ze moet dus sturen:

$$(c^{d_B} \pmod{n_B})^{e_A} \pmod{n_A} \equiv m$$

En Bob ontcijfert dan:

Voorbeeld:

Alice wil de boodschap '69' naar Bob sturen.

Ze verstuurt:

$(69^{24888081} (\text{mod } 9991163911))^{11111357} (\text{mod } 9998000099) \equiv 2264438400.$

Bob ontcijfert:

$(2264438400^{4264337} (\text{mod } 9998000099))^{123454321} (\text{mod } 9991163911) \equiv 69$

5.1.6 Opgaven

1. Laat zien dat het voorbeeld hierboven klopt.
2. Stel dat een afluisteraar een geheime niet van een handtekening voorziene boodschap onderschept. Ze heeft een algoritme dat per seconde 10^6 getallen uitprobeert om een boodschap uit $m^e \equiv c \pmod{n}$ te bepalen. Hoeveel jaar kan het kraken duren als n uit 200 cijfers bestaat?
3. Laat zien hoe Bob een boodschap 1000000001 van een handtekening kan voorzien en hoe Alice die controleert.

5.2 De veiligheid van RSA

Stel nu eens dat Eva, onze afluisteraar, de boodschap:

$$c \equiv m^{e_B} \pmod{n_B}$$

die voor Bob bestemd is onderschept. Hiermee kan ze het volgende doen:

1. Als Eva de geheime exponent d_B van Bob kent, kan ze m uit de cijfertekst c berekenen op precies dezelfde manier als Bob dat kan door $c^{d_B} \pmod{n_B}$ te bepalen.
2. Om d_B te bepalen uit de openbare exponent e_B en de vergelijking $e_B \cdot d_B \equiv 1 \pmod{\phi(n_B)}$ is ook makkelijk als ze $\phi(n_B)$ maar kent.
3. Om $\phi(n_B)$ te bepalen, moet ze de ontbinding van n_B in p_B en q_B achterhalen. Dit is voor kleine n_B niet moeilijk, maar naarmate n_B meer getallen bevat wordt dit steeds vervelender.

De uitvinders van RSA zeiden dat n ongeveer 200 cijfers lang moest zijn om factoriseren vrijwel onmogelijk te maken, maar in 1999 heeft een grote groep rekenaars, die via het internet verbonden waren, een getal van 512 bits ontbonden, dit is ongeveer 154 cijfers lang, want $2^{512} \approx 10^{154}$. Het RSA systeem met een modulus van 512 bits lang wordt momenteel op een aantal plaatsen in de wereld gebruikt, onder andere voor elektronische betaling over internet. Dat is dus niet meer aan te raden.

De veiligheid van het RSA systeem wordt dus bepaald door de stand van zaken op het gebied van factoriseren. Met andere woorden: hoe beter en hoe sneller we getallen kunnen factoriseren des te groter moeten de priemgetallen worden gekozen.

5.2.1 Opgaven

1. Een gebruiker van een RSA systeem heeft met veel moeite een priemgetal p gevonden en komt er per toeval achter dat ook $q = p + 12$ priem is. Hij kiest als modulus hun product dat gegeven wordt door $n = 4606061759128693$. Hoe groot zijn p en q?

Verder...

Op het internet zijn veel interessante dingen te vinden over crypografie. In de tekst is hier al enkele malen naar verwezen, maar sites die we je niet willen onthouden zijn:

http://www.trincoll.edu/depts/cpsc/cryptography/
http://www.orst.edu/dept/honors/makmur/alice.html
http://my.netian.com/~dubs37/english/
http://price.cnchost.com/notes/index.htm
http://www.pacificnet.net/~tgrupe/crypto.htm

Veel 'lees'- en 'doe'- plezier!

Literatuurlijst

- Fundamentals of Cryptology; A Professional Reference and Interactive Tutorial, Kluwer Academic Publischers – *H.C.A. van Tilborg*

Docentenhandleiding

"Kun je de code kraken"

Technische Universiteit Eindhoven
M.M.C. Tuyp
April 2002

Inleiding

Het boekje 'Kun de de code kraken?' is een bewerking van de masterclass informatiebeveiliging gegeven op 22 maart 2000 door Prof. Dr. H.C.A. van Tilborg. De bewerking is gemaakt door Mw. M.M.C. Tuyp, student wiskunde aan de TU/e en docent wiskunde aan B.C. Broekhin te Roermond.

De meeste leerlingen gaan dagelijks om met een computer. Ze hebben e-mail, chatten en bestellen soms zelf goederen via het internet. Ook weten een heleboel van deze leerlingen hoe ze al dan niet illegaal het een en ander moeten 'downloaden' en 'uploaden'. Daarnaast bezitten de meesten een bankpasje en misschien zelfs nog andere zogenaamde 'plastic' betaalkaarten en identietijdspasjes die ze regelmatig gebruiken. Er vindt bij deze handelingen een heleboel informatieuitwisseling plaats en het is natuurlijk belangrijk dat dit op een veilige manier gebeurt. Er zijn daarom technieken ontwikkeld om informatie die langs elektronische weg wordt verstuurd te coderen. Achter dit coderen zit veel wiskunde. Dit noemen we cryptografie.

De reader 'Kun je de code kraken' verteld over de technieken van het coderen en over de wiskunde die hierachter zit. Het materiaal is geschikt om te lezen, enige opgaven te maken[1] en zelf aan de hand van diverse suggesties die in het boekje worden gegeven enig onderzoek te doen.

Doel

Cryptografie is, tenzij een leerling zich daar zelf heeft in verdiept, een onbekend onderwerp. Modulorekenen is onbekend. Daarentegen wordt wel uitvoerig ingegaan op exponentiële functies en logaritmen. Dit onderwerp kan als een uitbreiding op die stof worden gezien. Als een leerling niet alle opdrachten maakt zal een onderzoek moeten worden uitgevoerd. In de reader worden tal van interessante internetsites gegeven waar voldoende te vinden is. Na het doorwerken van de reader moeten de leerlingen:

- Enkele cryptosystemen kennen, hierover in hun eigen bewoordingen kunnen vertellen en het systeem eventueel aan een andere leerling kunnen uitleggen
- ggd van twee getallen kunnen bepalen
- Simpele modulo opgaven kunnen maken
- De kleine stelling van Fermat kennen
- De stelling van Euler kennen
- Euler ϕ kennen en de formule van Euler voor $\phi(n)$ kennen en kunnen uitleggen waarom dit zo is
- Het grondidee achter cryptosystemen met openbare sleutels kunnen uitleggen aan de hand van een simpel voorbeeld
- Iets kunnen vertellen over de veiligheid van RSA.

[1] Als alle opgaven in de Reader worden gemaakt, waaronder ook het maken van kleine programmaatjes valt, is het de vraag of een leerling dan al niet dusdanig diep met het onderwerp is bezig geweest en zoveel uren heeft besteed, dat bijna aan de eisen van een profielwerkstuk is voldaan. Hierbij moet dan wel een logboek worden bijgehouden en dienen de gemaakte programmaatje te worden bijgevoegd, dan wel gedemonstreerd.

Doelgroep en vereiste voorkennis

Dit onderwerp is geschikt voor leerlingen uit de klassen 5 en 6 VWO met profiel N&G of N&T. Enige voorkennis op het gebied van exponentiële en logaritmische functies is gewenst.

Tijdsduur

De tijdsduur van het doornemen van het boekje zal afhangen van het aantal gemaakte opgaves. Een minimum van 20 uur kan wel worden aangenomen.

Benodigde Materialen

Computer en/of GR. Een programma als Excell heeft voldoende mogelijkheden om een en ander op te lossen.

Gewenste begeleiding

In theorie is het boekje 'Kun je de code kraken?' zo opgebouwd dat de leerling met zelfstudie en het maken van de opgaven alsmede wat onderzoek op het internet geen extra begeleiding nodig heeft. Mogelijk is wat hulp vereist bij het nieuw ingevoerde onderwerp 'modulo rekenen'.

Opmerkingen

Bij het onderwerp over de Vigenère staat op pagina 14 een link verkeerd afgedrukt. Dit moet zijn:

http://www.cs.arizona.edu/people/math/Cipher/query_vcb.html.

In de berekening $52331 \cdot 36151 \cdot 30198 \cdot 36 \cdot 6 \equiv 24455 (\text{mod}\, 99991)$ op pagina 29 staat een tikfout. Het antwoord moet zijn $34455 (\text{mod}\, 99991)$.

Kun je die code kraken?

Antwoorden

2.1.1

1. jlozcyfyh
2. 20, het woord was "meesterklas"
3. a) $237 \pmod{11} \equiv 6$
   b) $1496 \pmod{9} \equiv 2$
   c) $-401 \pmod{7} \equiv 5$
4. Het omzetten van tekst naar cijfers gaat heel makkelijk in een programma als Excell waarin deze functie bestaat, alsook het omzetten van getallen naar tekst.
5. PROGRAM: MOD
   : Prompt A,B
   : A – int(A/B)*B → M
   : Disp A, "MOD", B, "IS", M
   : Delvar A
   : Delvar B
   : Delvar M
   :
6. * Zie opgave 4.

2.2.1

Er zijn 26! mogelijke sleutels bij enkelvoudige substitutie.

2.2.3

1. the frequency of the various letters in a text makes it doable to break many a cryptosystem

2.3.3

1. To be or not to be that is the question. De gebruikte sleutel was: relations
2. If signals are to be displayed in the presence of an enemy, they must be guarded by ciphers. The ciphers must be capable of frequent changes. The rules by which these changes are made must be simple. The ciphers are undiscoverable in proportion as their changes are frequent and as the messages in each change are brief. From Albert J. Meyers's Manual of Signals.

   Het gebruikte sleutelwoord was SIGNAL

2.4

De machine is na 26^3 vercijferingen terug in de oorspronkelijke stand.

Een nadeel van de reflector is dat geen enkel karakter ooit op zichzelf kan worden afgebeeld, hiervan kunnen diegenen die de code proberen te breken gebruik maken.

2.5.1

Het aantal sleutels verdubbelt bij elke bit die wordt toegevoegd. Het aantal sleutels bij AES met 128 bits is 2^{120}.

3.1.1

1. 25
2. ggd(610, 987) = 1

   987 = 1 × 610 + 377
   610 = 1 × 377 + 233
   377 = 1 × 233 + 144
   233 = 1 × 144 + 89
   144 = 1 × 89 + 55
   89 = 1 × 55 + 34
   55 = 1 × 34 + 21
   34 = 1 × 21 + 13
   21 = 1 × 13 + 8
   13 = 1 × 8 + 5
   8 = 1 × 5 + 3
   5 = 1 × 3 + 2
   3 = 1 × 2 + 1
   2 = 2 × 1 + 0

   de lineaire combinatie is:
   -377·610 + 233·987 = 1

   ggd(2382, 237) = 3
   2382 = 10 × 237 + 12
   237 = 19 × 12 + 9
   12 = 1 × 9 + 3
   9 = 3 × 3 + 0

   de lineaire combinatie is:
   20·2382 - 201· 237 = 3
3. 99
4. PROGRAM: GGD
   : Prompt A,B
   : A→X
   : B→Y
   : While B≠0
   : A – int(A/B)*B→C
   : B→A
   : C→B
   : End
   : Disp "GGD ", X, "EN ",Y, "IS",A
   : Delvar A
   : Delvar B
   : Delvar C
   : Delvar X
   : Delvar Y
   :
5. *

3.3.1

1. $\phi(15) = 8$, $\phi(35) = 24$
2. *
3. *
4. A = {1, 2, 4, 7, 8, 11, 13, 14}
   B = 4·{1, 2, 4, 7, 8, 11, 13, 14}= {4, 8, 16, 28, 32, 44, 52, 56}
   B (mod 15) = {4, 8, 1, 13, 2, 14, 7, 11}
   dus $4\cdot1\cdot4\cdot2\cdot4\cdot4\cdot4\cdot7\cdot4\cdot8\cdot4\cdot11\cdot4\cdot13\cdot4\cdot14 \equiv 1\cdot2\cdot4\cdot7\cdot8\cdot11\cdot13\cdot14 \pmod{15}$
   $\Leftrightarrow 4^8\cdot1\cdot2\cdot4\cdot7\cdot8\cdot11\cdot13\cdot14 \equiv 1\cdot2\cdot4\cdot7\cdot8\cdot11\cdot13\cdot14 \pmod{15}$
   $\Leftrightarrow 4^8 \equiv 1 \pmod{15}$
5. 12
6.

moge-lijk	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
weg					5					10					15					20					25					30
weg			3			6			9			12			15			18			21			24			27			30
dubbel weg															**15**															**30**
weg		2		4		6		8		10		12		14		16		18		20		22		24		26		28		30
dubbel weg						**6**				**10**		**12**						**18**		**20**				**24**						**30**
over	1						7				11		13				17		19				23						29	

   $\phi(30) = 30 - 6 - 10 + 2 - 15 + 7 = 8$
7.
   a) $\phi(126) = 36$
   b) $\phi(1265) = 880$
   c) $\phi(215689) = 215688$
   d) $\phi(369879) = 244536$
8. $\phi(n) = \phi(p^a)\,\phi(q^b)\phi(r^c)\phi(s^d) = p^{a-1}q^{b-1}r^{c-1}s^{d-1}\cdot(p-1)(q-1)(r-1)(s-1) =$
   $p^a q^b r^c s^d \cdot (1 - 1/p)(1 - 1/q)(1 - 1/r)(1 - 1/s) = n\cdot(1 - 1/p)(1 - 1/q)(1 - 1/r)(1 - 1/s)$
9. a) $x = 70\cdot u + 37$
   b) $t = 60\cdot z + 15$

3.4.1

1. a) 11001111000110
   b) 101000011010
   c) 10000000101101011

2. a) 87
   b) 246

5.1.6

1. $69^{24888081} (\text{mod } 9991163911) \equiv 7663137819$
   $7663137819^{11111357} (\text{mod } 9998000099) \equiv 2264438400$
   $2264438400^{4264337} (\text{mod } 9998000099) \equiv 7663137819$
   $7663137819^{123454321} (\text{mod } 9991163911) \equiv 69$
2. Als n uit 200 cijfers bestaat heeft dit als wetenschappelijke notatie de vorm $g \cdot 10^{200}$, met $0 < g < 10$. De afluisteraar moet dus $g \cdot 10^{200}$ getallen uitproberen. Als hij per seconde 10^6 getallen kan uitproberen doet hij daar dus $g \cdot 10^{194}$ seconden over. Er zitten $3{,}1536 \cdot 10^7$ seconden in een jaar. Het kan dus ongeveer 10^{187} jaar duren voordat de code wordt gekraakt.
3. $m^{d_B} (\text{mod } n_B) \equiv c$, dus $1000000001^{42643373} (\text{mod } 9998000099) \equiv 1026322290$

   $c^{e_B} (\text{mod } n_B) \equiv m$, dus $1026322290^{11111357} (\text{mod } 9998000099) \equiv 1000000001$

5.2.1

1. De getallen zijn 67867979 en 67867967.

Kun je me de kortste weg vertellen?

Inhoudsopgave

Combinatorische Optimalisering

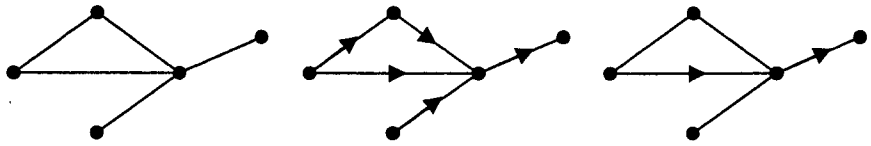
28 november 2000

1 Grafen

Dit boekje is een bewerking van de masterclass combinatorische optimalisering: "Kun je me de kortste weg vertellen?", gegeven op 5 maart 1999 door Prof.dr.J.K. Lenstra in samenwerking met Dr.ir. C. Hurkens.

1.1 Wat is een graaf?

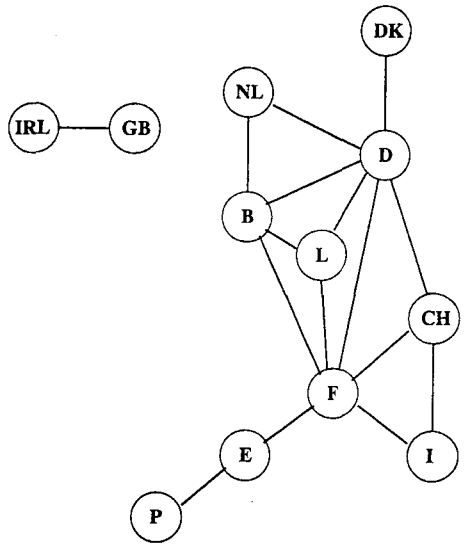
Een graaf is een tekening die alleen bestaat uit punten en verbindingslijnen. De verbindingslijnen noemen we kanten. (Andere benamingen die je wel eens tegenkomt zijn knooppunten en wegen.) Een kant verbindt twee punten en een kant tussen de punten i en j geven we aan met ij. Soms heeft een kant een richting en loopt van i naar j. Dit schrijven we als $i \rightarrow j$. In figuur 1 zie je een **ongerichte** graaf, een **gerichte** graaf en een **gemengde** graaf. Een **gerichte** graaf is een graaf met pijlen in de kanten. Deze pijlen geven een verband tussen de (knoop)punten aan, b.v. 'Wie is de afstammeling van wie?' of 'Wie heeft gewonnen van wie?' Een **gemengde** graaf is een combinatie van een gerichte en een ongerichte graaf.



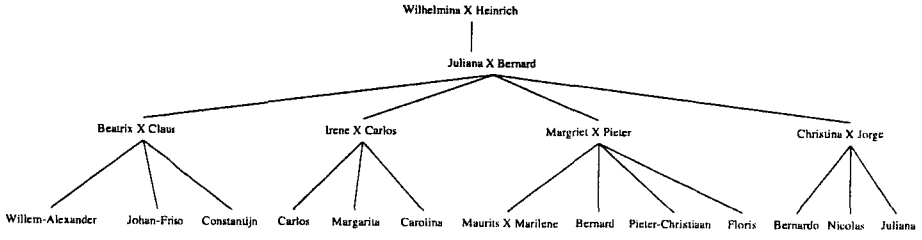
Figuur 1: Grafen

Met grafen kun je allerlei situaties beschrijven. Het gaat dan om situaties waarin er tussen **objecten**, voorgesteld door de punten, **paarsgewijze relaties** bestaan, voorgesteld door de kanten. In figuur 2 zie je bijvoorbeeld een graaf waarvan de punten twaalf landen in West-Europa zijn. Een kant ij geeft aan dat de landen i en j aan elkaar grenzen. In figuur 3 zie je een gerichte graaf die de afstamming van een persoon P tot in het derde voorgeslacht uitbeeldt. Een

kant $i \rightarrow j$ geeft hier aan dat j een kind is van i.



Figuur 2: Grenzen in West-Europa



Figuur 3: Stamboom

Een graaf die een bepaalde situatie beschrijft noemen we een **model** van die situatie. In een model neem je alleen de gegevens van een situatie op die belangrijk zijn voor het probleem dat je wilt oplossen.

Vragen die je bijvoorbeeld met grafen kunt oplossen zijn:

Als de punten van de graaf plaatsen zijn en de kanten zijn wegen tussen die plaatsen,
(1) hoe vind je dan een kortste netwerk dat alle plaatsen met elkaar verbindt?
(2) hoe vind je dan een kortste weg tussen twee gegeven plaatsen?

(3) hoe vind je een kortste route die langs alle plaatsen gaat?

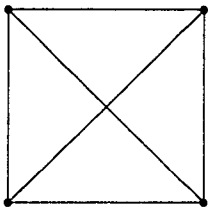
Je zult zien dat je, als je deze vragen kunt beantwoorden, ook problemen kunt oplossen die op het eerste gezicht niets met wegennetwerken te maken hebben. Je kunt namelijk veel andere problemen voorstellen als een wegennetwerk. Deze kun je dan ook weer met behulp van een graaf proberen op te lossen. Het is zelfs zo dat verschillende situaties tot hetzelfde model kunnen leiden.

1.2 Opgaven

1. Verzin zelf 3 voorbeelden van situaties die je als graaf kunt weergeven en teken die grafen.

2. Kun je situaties verzinnen die tot hetzelfde model leiden als de grafen die je bij 1. hebt getekent?

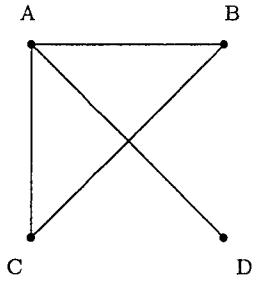
3. Een graaf heet **volledig** als elk punt in de graaf verbonden is met alle andere punten in de graaf. Hieronder zie je de volledige graaf met 4 punten.

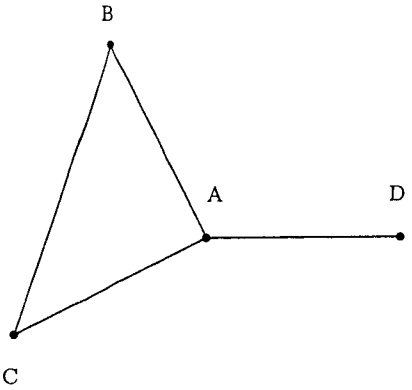


   (a) Teken de volledige graaf met 6 punten.

   (b) Hoeveel kanten heeft een volledige graaf met n punten?

4. Hieronder zie je twee gelijke grafen.

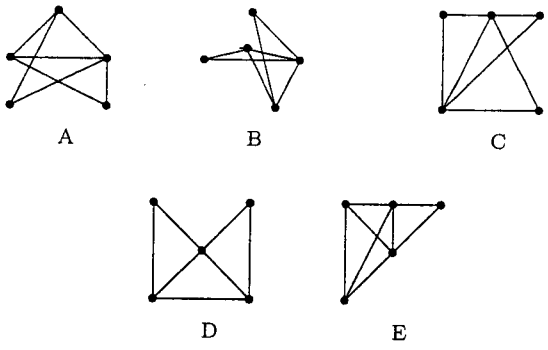




Twee grafen zijn gelijk als ze dezelfde (knoop)punten hebben en als tussen dezelfde punten evenveel kanten lopen die, indien we het over een gerichte

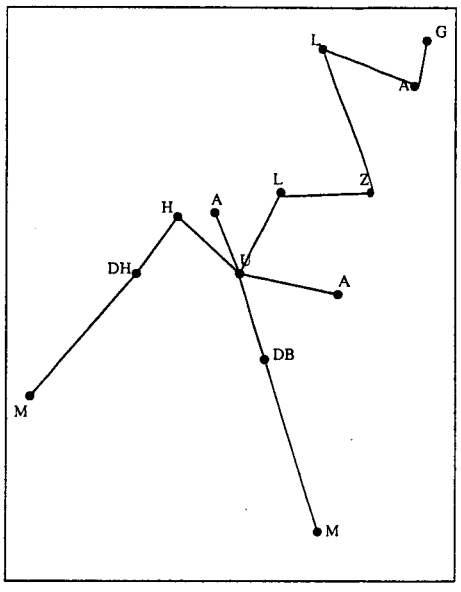
graaf hebben, dezelfde richting hebben.

Welke van de volgende grafen komen met elkaar overeen?



2 Kortste bomen

Hoe vind je een kortste wegennetwerk dat alle plaatsen met elkaar verbindt? Verbinden wil zeggen dat je vanuit elk punt ieder ander punt(eventueel via andere punten) kunt bereiken. Als voorbeeld nemen we een probleem met dertien plaatsen: Amsterdam en de twaalf Nederlandse provinciehoofdsteden. Een mogelijk netwerk zie je in figuur 4.



Figuur 4: Een wegennetwerk in Nederland

Hoe bepaal je nu het kortste netwerk? We maken hiervoor een model waarbij we een ongerichte graaf gebruiken. De steden stellen we als punten voor en de wegen tussen die steden als kanten. De afstanden tussen twee steden i en j noemen we dan c_{ij}. Kant ij heeft dus een **lengte** c_{ij}.

Voorbeeld
Als i = Amsterdam en j = Den Haag, dan is c_{ij} de afstand tussen Amsterdam en Den Haag.

Ook als we het over andersoortige problemen hebben, b.v. leeftijdsverschillen, hebben we het nog steeds over **lengte** c_{ij}. We nemen aan dat $c_{ij} \geq 0$ voor alle ij: de lengtes zijn niet-negatief.

Een reeks kanten ij, jk, kl, lm, ... die op elkaar aansluiten noemen we een **pad**. Een gesloten pad, waarvan het beginpunt en het eindpunt samenvallen,

heet een **circuit**.

Voorbeeld
Als i = Amsterdam, j = Den Haag, k = Utrecht en l = Lelystad, dan is ij, jk, kl, li het circuit Amsterdam-Den Haag-Utrecht-Lelystad-Amsterdam.

Je kunt meerdere circuits binnen een graaf hebben.

Een netwerk dat alle punten met elkaar verbindt en geen circuits bevat heet een **boom**. In een boom is er tussen elk tweetal punten precies één pad. En een boom op 13 punten bestaat uit 12 kanten.

Het netwerk waar je naar op zoek bent bevat natuurlijk geen circuits.

Vraag:
Waarom kan zo'n netwerk geen circuits hebben?

2.1 Het 'Greedy' Algoritme

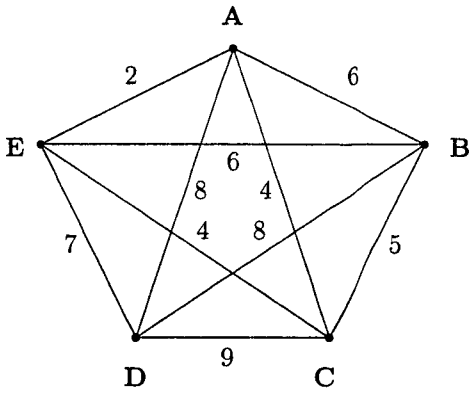
Je zoekt dus naar een boom die zo is opgebouwd dat als je alle lengtes van zijn kanten bij elkaar optelt, je een zo klein mogelijk getal krijgt. We noemen dit een kortste boom. Hiervoor bestaat een **algoritme**. (Een algoritme is een soort recept van hoe je iets moet doen). Dit algoritme ziet er als volgt uit:

1. Kies een willekeurig punt i in je graaf als begin van je netwerk.

2. Als je netwerk nog niet alle punten bevat, bepaal dan twee punten k en j, met j in het netwerk en k niet, waarvoor c_{jk} minimaal is. Voeg de kant kj aan het netwerk toe. Als er meerder mogelijkheden zijn dan kies je er een willekeurig.

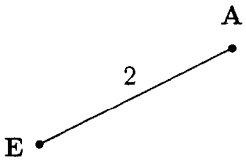
Dit algoritme noemen we het 'Greedy' Algoritme.

2.1.1 Voorbeeld van het 'Greedy' Algoritme.

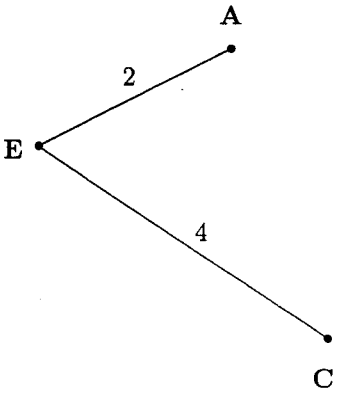


Stap 1.
Kies het "willekeurige punt" A.

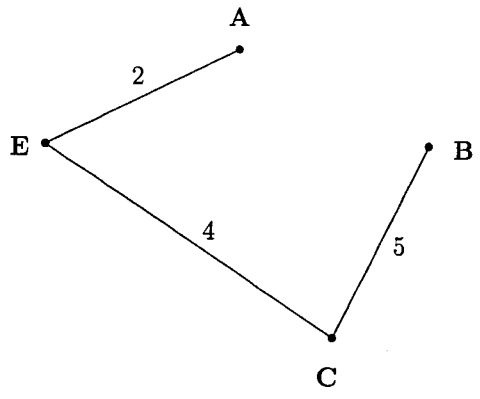
Stap 2.
De kant AE heeft de kleinste **lengte**. Deze kant moet je dus toevoegen.



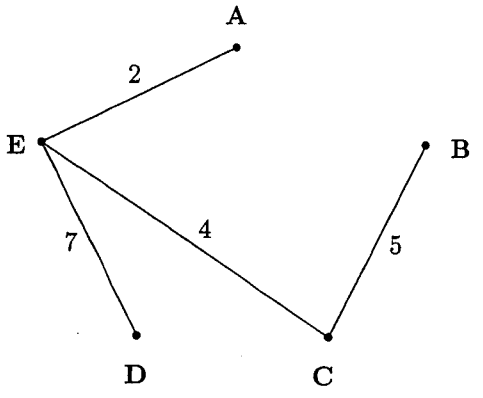
Stap 3.
Vervolgens pakken we de kant met de op één na kleinste **lengte**. We hebben er twee, namelijk AC of CE met **lengte** 4. Kies bijvoorbeeld CE.



Stap 4.
Nu kunnen we AC niet meer in onze boom opnemen, want dat zou een circuit opleveren. De daaropvolgende kant met de kleinste **lengte** is BC met **lengte** 5.

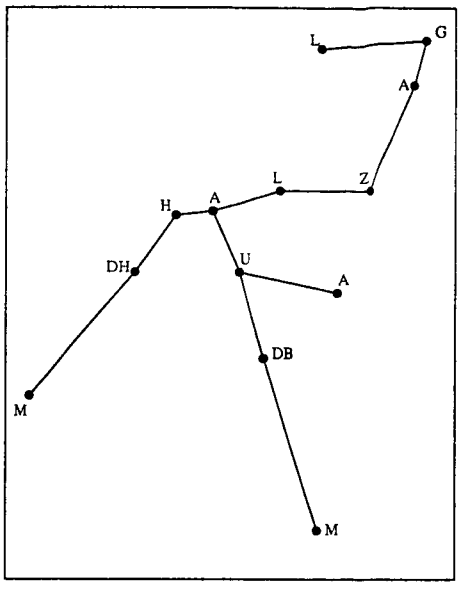


Stap 5.
Hierna zouden de kanten AB en BE in aanmerking komen, maar deze leveren ook beide een circuit, dus kiezen we kant DE met **lengte** 7. Hiermee hebben we een kortste opspannende boom gecreëerd met **lengte** 18.



Opmerking:
Als we bij de tweede Stap AC hadden genomen in plaats van CE dan hadden we een andere kortste opspannende boom gekregen, maar de **lengte** is dan nog steeds 18.

Als je dit algoritme op de steden van Nederland toepast dan krijg je de oplossing die je hieronder ziet.



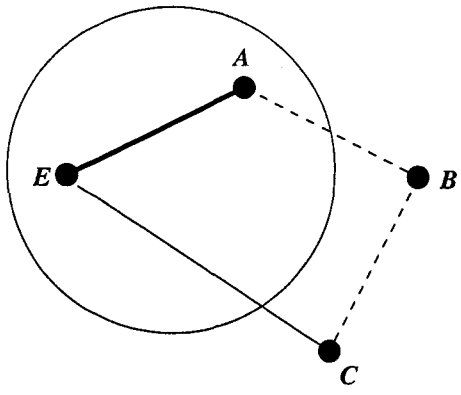
Figuur 5: Kortste wegennetwerk in Nederland

2.2 Bewijs van het 'Greedy' Algoritme

Geeft dit algoritme, dat het "Greedy" Algoritme genoemd wordt, nu echt de kortste boom? Ja, en dit kunnen we ook laten zien. Laten we nog eens bij stap (1) beginnen. Stap 1 is het kiezen van een punt, i. Dit punt zit zeker in de kortste boom, want alle punten van de graaf moeten in de kortste boom zitten. Nu kies ik een punt j uit de graaf dat de kortste afstand heeft tot punt i van alle punten in de graaf. De boom bestaande uit die twee punten is de kortst mogelijke boom tussen die twee punten binnen onze graaf. Vervolgens kiezen we een punt k dat de kortste afstand heeft tot punt i of punt j van alle punten in de graaf, uitgezonderd i en j natuurlijk, want die zitten al in je boom. Na toevoegen van punt k met de bijbehorende kortste kant is de boom die uit drie punten bestaat nog steeds de kortste boom tussen die drie punten. Zo kunnen we verder gaan, totdat we alle punten hebben gehad. De enige voorwaarde waar je aan moet houden is dat je geen circuits mag maken.(zie voorbeeld 2.1.1.)

Stel eens dat je kijkt naar het stukje boom dat in stap 2 van je algoritme af is. Dit is een netwerk op een gedeelte van alle punten in de graaf (een **deelverzameling** van de verzameling van alle punten in je graaf). In het voorbeeld zijn dit de punten A en E met kant AE. Dit netwerk zit ook in een kortste boom op je hele graaf. We kiezen nu op grond van het algoritme de twee punten C en E; C zit nog niet in je netwerk, E wel. Veronderstel nu eens dat de kant CE niet in je kortste boom zit. Dan moet C via een ander pad met je netwerk verbonden zijn. In dit pad zit een kant, bijvoorbeeld AB, met A in je netwerk

en B niet, waarvan we zeker weten dat $c_{AB} \geq c_{CE}$, anders konden we E en C niet zo kiezen in stap 2, dus mogen we c_{AB} door c_{CE} vervangen.



Figuur 6: Waarom de boom niet korter kan

2.3 Opgaven

1. Teken alle verschillende kortste bomen bij voorbeeld 2.1.

2. In de volgende tabel zie je de afstanden (in mijlen) tussen zes plaatsen in Ierland. Teken een graaf en gebruik het "Greedy" Algoritme om een kortste boom te vinden die deze plaatsen verbindt.

	Athlone	Dublin	Galway	Limerick	Sligo	Wexford
Athlone	-	78	56	73	71	114
Dublin	78	-	132	121	135	96
Galway	56	132	-	64	85	154
Limerick	73	121	64	-	144	116
Sligo	71	135	85	144	-	185
Wexford	114	96	154	116	185	-

3. Een inbraakalarm is weergegeven in de vorm van een graaf waarvan de kanten gemaakt zijn van zeer kostbaar koperdraad. Elke kant heeft een verschillende waarde (=**lengte**). Het alarm gaat af als de graaf niet verbonden is. Een inbreker wil zoveel mogelijk van het kostbare koperdraad stelen. Welke kanten moet hij weghalen om een maximale buit binnen te krijgen?

4. Laat zien hoe je het "Greedy" Algoritme moet aanpassen om een langste opspannende boom te creëren.

5. Maak bij de volgende tabellen een graaf en zoek hierbij een kortste en een langste opspannende boom.

	Berlijn	Londen	Madrid	Moscou	Parijs	Rome
Berlijn	-	7	15	11	7	10
Londen	7	-	11	18	3	12
Madrid	15	11	-	27	8	13
Moscou	11	18	27	-	18	20
Parijs	7	3	8	18	-	9
Rome	10	12	13	20	9	-

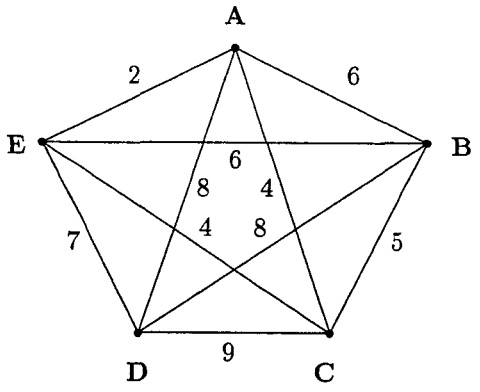
	Aberd.	Edinb.	F.W.	Glasg.	Inv.	Perth
Aberdeen	-	120	147	142	104	81
Edinburgh	120	-	132	42	157	45
Fort William	147	132	-	102	66	105
Glasgow	142	42	102	-	168	61
Inverness	104	157	66	168	-	112
Perth	81	45	105	61	112	-

2.4 Algoritme van Prim-Dijkstra

Het 'Greedy' Algoritme is makkelijk met de hand toe te passen als je een kleine graaf hebt. Om het door een computer te laten doen is echter moeilijker. Je wilt steeds de kanten ordenen op aflopende lengte en je moet steeds kijken of er geen circuit ontstaat. Door een kleine aanpassing in het "Greedy" Algoritme is dit op te lossen. Het algoritme dat dan overblijft is beter bekend als het "Algoritme van Prim-Dijkstra" en loopt als volgt:

1. Je maakt eerst een tabel van alle kanten tussen de knopen in je graaf.
2. Neem nu een willekeurige knoop in je graaf. Deze komt in de boom die je wilt creëren. Stel je kiest B.
3. Verwijder nu rij B uit je tabel en zoek in kolom B de kleinste waarde op.
4. Kijk welke knoop bij deze kleinste waarde hoort. Stel dat is knoop C.
5. Voeg dan kant BC aan je boom toe.
6. Verwijder rij C uit je tabel en zoek nu in de kolommen B en C naar de kleinste waarde.
7. Herhaal nu vanaf stap 4, waarbij je steeds bij één kolom meer naar de kleinste waarde moet zoeken.
8. Als je geen rijen meer over hebt in je tabel heb je een kortste boom gevonden.

2.4.1 Voorbeeld van het Algoritme van Prim-Dijkstra



Stap 1.
Bij de graaf in de bovenstaande figuur hoort de volgende tabel:

	A	B	C	D	E
A	-	6	4	8	2
B	6	-	5	8	6
C	4	5	-	9	4
D	8	8	9	-	7
E	2	6	4	7	-

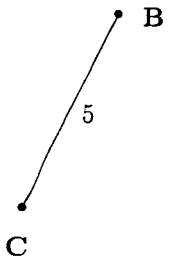
Stap 2.
Kies B om je boom mee te beginnen.

• **B**

Stap 3.
Ik moet nu dus **rij** B uit de tabel verwijderen en de kleinste waarde in **kolom** B opzoeken.

	A	B	C	D	E
A	-	6	4	8	2
C	4	[5]	-	9	4
D	8	8	9	-	7
E	2	6	4	7	-

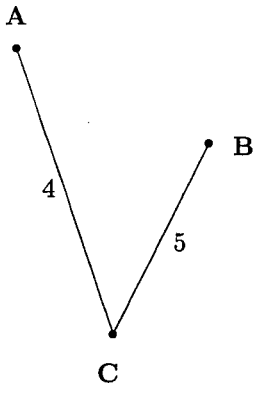
Stap 4 en 5.
Uit de tabel blijkt nu dat BC de kant is met de kleinste **lengte**, dus voeg je kant BC en knoop C aan je boom toe.



Stap 6.
Nu moet je **rij** C uit de tabel halen en de kleinste waarde in **kolom** B of **kolom** C opzoeken.

	A	B	C	D	E
A	-	6	[4]	8	2
D	8	8	9	-	7
E	2	6	[4]	7	-

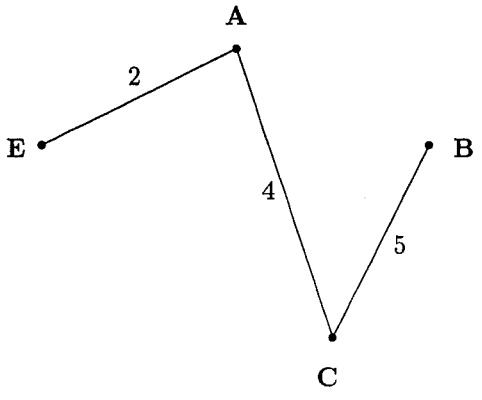
Stap 7
CA en CE zijn de volgende kanten met de kleinste **lengte**, waardoor je boom groter kan worden. Kies daar ééntje van, CA. De boom wordt uitgebreid met kant CA en knoop A.



Stap 8.
Rij A haal je uit de tabel en de kleinste waarde die je vindt onder de **kolommen** B, C en A is die in rij E, nl.: 2.

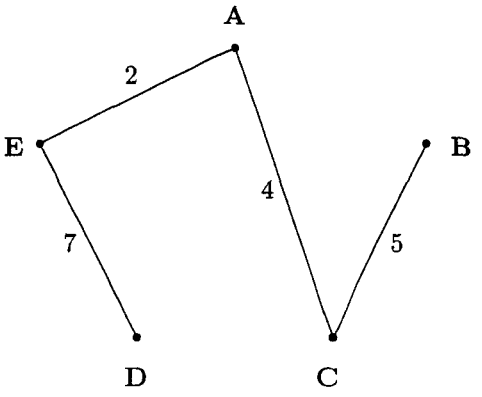
	A	B	C	D	E
D	8	8	9	-	7
E	[2]	6	4	7	-

Stap 9.
Vergroot je boom met kant AE en knoop E en haal **rij** E uit je tabel.

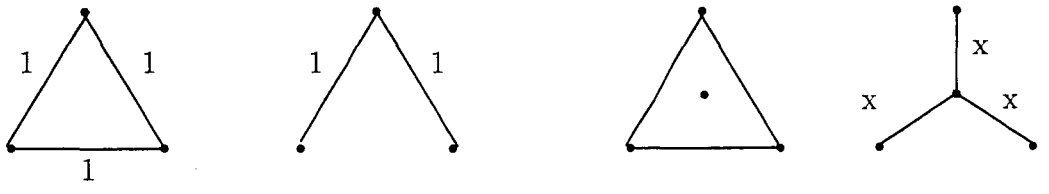


	A	B	C	D	E
D	8	8	9	-	[7]

Stap 10.
In de **kolommen** A, B, C en E vind je nu onder E de kleinste waarde. De laatste kant die je aan mijn boom plakt is dus kant ED, waarmee je dan tegelijk als laatste knoop D toevoegt. Alle knopen van de originele graaf komen voor in de boom en dit is een kortste opspannende boom van de graaf.



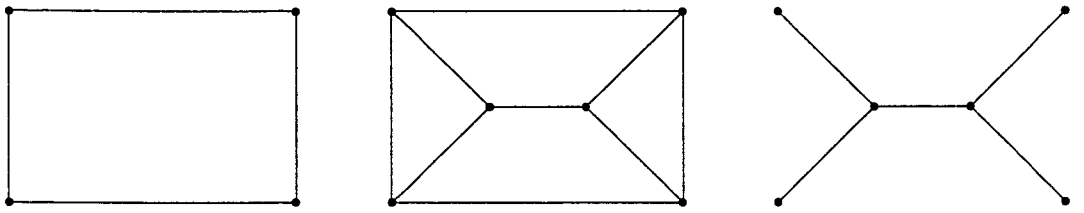
N.B.:
Er zit nog een addertje onder het gras. De boom bestaat uit kanten van de oorspronkelijke graaf. Dat wil zeggen: je mag alleen wegen aanleggen die gegeven plaatsen, dus werkelijke punten uit je graaf, met elkaar verbinden. Als de plaatsen nu eens liggen op de hoeken van een gelijkzijdige driehoek, dan bestaat de boom uit twee van de drie zijden. Maar het is voordeliger een nieuwe plaats te creëren, in het middelpunt van de driehoek, en die met de drie gegeven plaatsen te verbinden. Door punten toe te voegen kun je ook de boom in figuur 5 nog flink verbeteren. Je zoekt dan naar een kortste **Steiner-boom**. Hieronder zie je de Steinder-boom bij een gelijkzijdige driehoek.



2.5 Opgaven

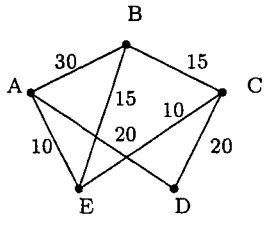
1. Los opgaven 2 t/m 5 uit 2.3 op met behulp van het "Algoritme van Prim-Dijkstra".
2. Bepaal de lengte van de Steiner-boom in het voorbeeld van de gelijkzijdige driehoek.

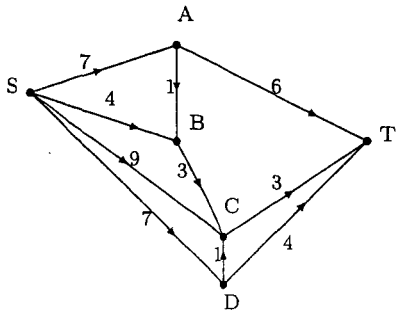
3. Hieronder zie je een graaf op vier punten, met daarnaast de overstap naar de bijbehorende Steiner-boom. Bepaal de positie van de punten.



3 Kortste paden

Er bestaat ook een algoritme waarmee je het kortste pad tussen twee plaatsen kunt vinden. Dat algoritme is vrij ingewikkeld en moet je alleen gebruiken bij grote grafen. Het kortste pad in de linkergraaf tussen A en B is AEB, dat zie je zo. Maar een kortste pad tussen S en T in de rechtergraaf is niet zomaar te zien.

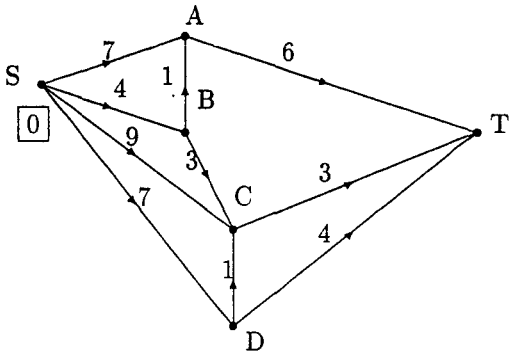




Voordat we het algoritme formuleren passen we het eerst toe met de rechtergraaf als voorbeeld.

3.1 Een algoritme om een kortste pad te vinden

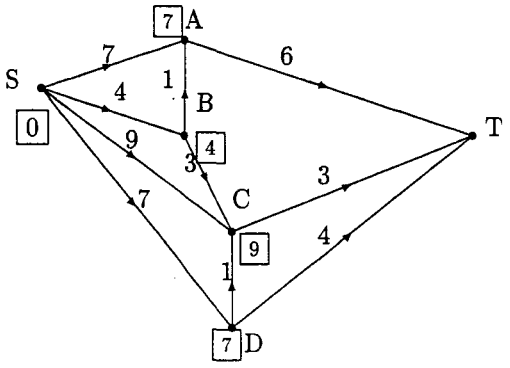
In het hieronderstaande netwerk zoeken we het korste pad van S naar T. Om niet in de war te raken door alle getalletjes die in je graaf komen te staan, stop je alle gegevens die je verzakelt tijdens het zoeken naar het kortste pad in een tabel.



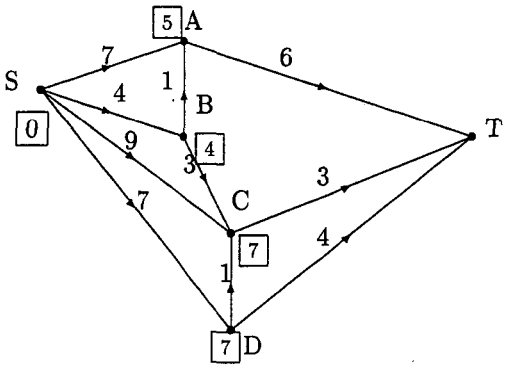
S noemen we punt **1**. De lengte tot nu toe geef je aan met $L(1)$. $L(1)$ is dus 0. De eerste rij in je tabel geeft je de naam van de knoop of knopen die net een lengte hebben gekregen. De eerste rij in je tabel wordt in dit geval dus rij S.

knopen	S	A	B	C	D	T
S	0	7	4	9	7	...

Nu kijk je naar knopen die je via één kant vanuit S kunt bereiken. In dit geval zijn dat A, B, C en D. Deze krijgen nu elk een merk, een voorlopige bovengrens van S naar die punten, $M(A) = 7$, $M(B) = 4$, $M(C) = 9$ en $M(D) = 7$.

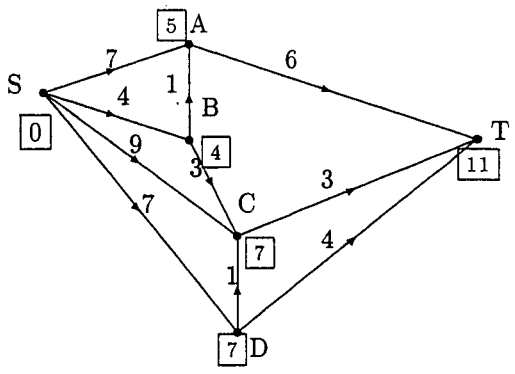


B is de knoop met het kleinste merk. B krijgt nu $L(B) = 4$ en de tweede rij in je tabel wordt rij B. Vervolgens kijk je naar de knopen die direct vanuit B bereikbaar zijn (A en C). De merken van deze knopen worden nu aangepast, $M(A) = 5$ en $M(C) = 7$. Dit verwerk je gelijk in je nieuwe tabel.



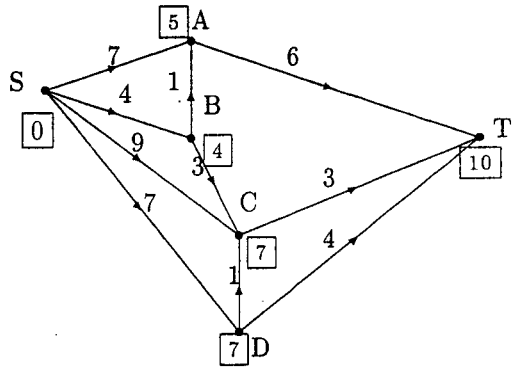
knopen	S	A	B	C	D	T
S	0	7	4	9	7	...
B		5	4	7	7	...

A heeft nu het kleinste merk, dus $L(A) = 5$. Dan kijk je naar de knopen direct bereikbaar vanuit A. Dit is alleen T. T krijgt $M(T) = 5 + 6 = 11$.



knopen	S	A	B	C	D	T
S	0	7	4	9	7	$\cdots$
B		5	4	7	7	$\cdots$
A		5		7	7	11

C en D hebben nog geen lengte. Ze hebben beide hetzelfde merk en er zijn geen knopen met een kleiner merk. De lengte van C en D wordt dus 7 en de volgende rij in je tabel wordt rij C, D. De enige direct bereikbare knoop vanuit deze punten is knoop T. Vanuit C wordt het merk van T gelijk aan 10 en vanuit D wordt het merk van T gelijk aan 11. We mogen het merk van T dus aanpassen, $M(T) = 10$. Je hebt nu gevonden:



knopen	S	A	B	C	D	T
S	[0]	7	4	9	7	...
B		5	[4]	7	7	...
A		[5]		7	7	11
C,D				7	7	10
T						[10]

Het kortste pad tussen S en T is $SBCT$. Hieronder vatten we het algoritme nog eens samen.

Het beginpunt van de graaf waarin je een kortste pad zoekt noemen we punt **1**. Dit punt ligt vast. Verder heeft elk punt i in de graaf een **merk** $M(i)$, de voorlopige bovengrens van een kortste pad van **1** naar i. $M(i)$ wordt in elke stap die we maken aangepast. Het punt i krijgt een **lengte** $L(i)$ als we op een gegeven moment bij punt i vanuit **1** zijn en $M(i)$ kan niet meer kleiner worden gemaakt. $M(i)$ wordt dan $L(i)$, dus:

1. We geven het beginpunt **1** een lengte $L(1) = 0$ en zeggen $j = 1$. Alle andere punten i krijgen een merk $M(i) = \infty$. Het punt j is op dit moment het laatste punt dat een lengte heeft gekregen, n.l. 0.

2. We kijken naar alle punten k die nog geen lengte hebben. Als er een kant jk bestaat waarbij $M(k) > L(j) + c_{jk}$, dan veranderen we $M(k)$ in $L(j) + c_{jk}$.

3. Nu kiezen we uit alle punten k dàt punt k^* dat het kleinste merk, $M(k^*)$, heeft en zeggen $L(k^*) = M(k^*)$ en $j = k^*$, dus j is weer het laatste punt dat een lengte heeft gekregen. Zolang er nog punten over zijn zonder lengte, herhalen we het algoritme vanaf punt 2.

Als je tijdens het toepassen van het algoritme ervoor kiest om alle gegevens die je verzamelt in een tabel te stoppen, doe je nog het volgende:

1. Boven elke kolom zet je de naam van een van de knopen in je graaf.

2. Vervolgens geef je de eerste rij de naam van een knoop of knopen die net een **lengte** hebben gekregen.

3. Zet die **lengte** in de gelijknamige kolom en omcirkel deze.

4. Om de rijen af te maken bekijk je de knopen die direct vanuit de net toegevoegde knoop bereikt kunnen worden en zetten daar de bijbehorende **merken** bij. In rij k onder kolom j moet dus $M(k) = L(j) + c_{jk}$ komen te staan.

5. Nu zoek je in de net gemaakte rij naar de kleinste waarde die géén **lengte** is. De knoop die boven de kolom staat waarin deze waarde voorkomt is

de naam van je volgende rij. Dit kunnen ook meerdere knopen zijn als er twee gelijke kleinste waarden in je onderzochte rij voorkomen. Dan zet je gewoon twee namen voor je volgende rij.

6. Herhaal vanaf 2 totdat je in je eindknoop van het pad dat je zoekt bent gekomen.

3.1.1 Voorbeeld van een kortste pad.

Kortste paden heb je niet alleen bij wegennetwerken. De tekst die je nu leest is gemaakt met het tekstverwerkingsprogramma LaTeX. Om een alinea in regels in te delen gebruikt LaTeXeen kortste pad algoritme, zie figuur 7. De punten in je graaf worden dan de plaatsen in de zin waar kan worden afgebroken. Als de tekst tussen twee punten i en j op één regel past, dan hebben we daar een kant ij. Hoe vervelender de afbreking des te groter is de lengte c_{ij} van deze kant. Het kortste pad dat LaTeXvindt geeft een alinea-indeling met het grootste leesgemak.

$|_0$De$|_3$ze $|_1$ tekst$|_1$ kan$|_1$ op$|_1$ der$|_2$tig$|_1$ plaat$|_2$sen$|_1$

wor$|_2$den$|_1$ af$|_2$ge$|_3$bro$|_3$ken.$|_0$ Som$|_3$mi$|_3$ge$|_1$ af$|_2$bre-$|_3$

kin$|_3$gen$|_1$ zijn$|_1$ le$|_3$lij$|_3$ker$|_1$ dan$|_1$ an$|_3$de$|_3$re.$|_1$

Figuur 7: Het kortste pad geeft de mooiste alinea

3.2 Opgaven

1. Maak van de volgende tabel een gerichte graaf. Zet de juiste lengtes bij de kanten en zoek een kortste pad tussen S en T.

	S	A	B	C	D	E	T
S	-	7	13	28	-	-	-
A	-	-	4	-	25	10	-
B	-	-	-	5	6	-	-
C	-	-	-	-	-	3	-
D	-	-	-	-	-	-	5
E	-	-	-	-	-	-	12
T	-	-	-	-	-	-	-

2. Een bedrijf heeft 5 vestigingen in 5 verschillende steden: A, B, C, D en E. De reiskosten tussen deze steden zie je in onderstaande tabel. Wat is de goedkoopste route tussen elk tweetal steden?

	A	B	C	D	E
A	-	50	40	25	10
B	50	-	20	90	25
C	40	20	-	10	25
D	25	90	10	-	55
E	10	25	25	55	-

3. Maak van de volgende tabel een graaf en zoek dan vanuit S de kortste route naar elk ander punt in de graaf.

	S	A	B	C	D	E	F	T
S	-	1	3	6	-	-	-	-
A	1	-	5	-	2	4	-	-
B	3	5	-	2	-	7	3	-
C	6	-	2	-	-	-	6	-
D	-	2	-	-	-	1	-	7
E	-	4	7	-	1	-	4	5
F	-	-	3	6	-	4	-	2
T	-	-	-	-	7	5	2	-

4. Kun je met behulp van de tabel in opgave 3 ook een langste route vinden?

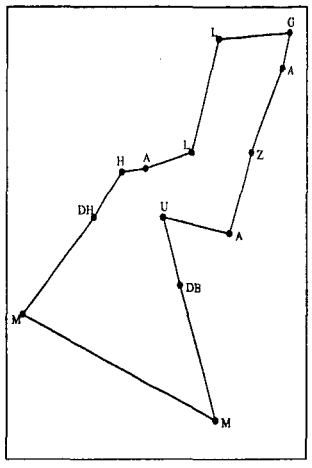
5. [1] Bewijs met **volledige inductie** (zie bijlage) dat je op de beschreven manier inderdaad een kortste pad vindt.

[1] Deze opgave is vrij pittig en kan desgewenst worden overgeslagen.

4 Kortste routes

4.1 Handelsreizigers

Een handelsreiziger moet vanuit zijn woonplaats een aantal andere steden bezoeken.'s Avonds wil hij weer zo vroeg mogelijk thuis zijn, dus moet hij een zo kort mogelijke route langs die steden zien te vinden. Hieronder zie je route van een handelsreiziger langs de provinciehoofdsteden schematisch weergegeven.



Figuur 8: Kortste route door 13 Nederlandse steden

Dit probleem kun je natuurlijk als een graaf voorstellen. De steden (ook de woonplaats van de handelsreiziger) zijn punten. De wegen tussen de steden zijn de kanten, die een lengte c_{ij} hebben die gelijk is aan het aantal kilometers dat je moet rijden tussen twee steden i en j. De vraag wordt dan een circuit te bepalen waarin je precies één keer langs ieder punt gaat, zodat de totale lengte, dus alle lengtes bij elkaar opgeteld, zo klein mogelijk is.

Een circuit dat elk punt van een graaf precies éénmaal bezoekt heet een **Hamiltoncircuit**. Bij het handelsreizigersprobleem zoeken we in een graaf met lengtes op de kanten naar een kortste Hamiltoncircuit.

Het handelsreizigersprobleem kun je in allerlei situaties toepassen. Hier volgen een aantal voorbeelden:

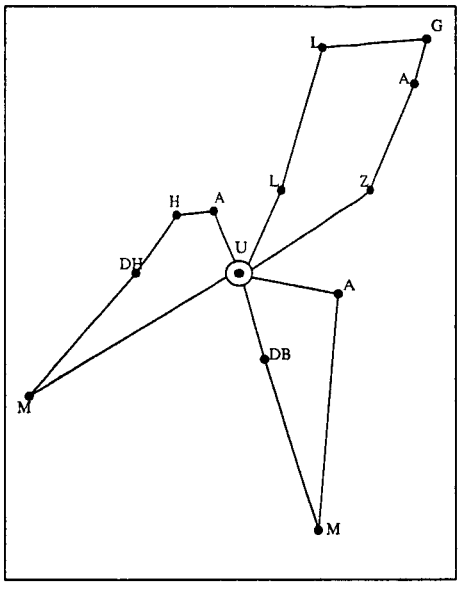
4.1.1 Voorbeelden van het handelsreizigersprobleem.

1. De handelsreiziger woont in New York en moet elke plaats in de V.S. van Amerika met tenminste 500 inwoners bezoeken. Hij mag niet verwachten

dat hij dezelfde avond weer thuis is: zijn probleem heeft 13.509 steden. Het is het grootste probleem van dit soort waarvoor een kortste route bekend is. Je ziet hem in figuur 9.

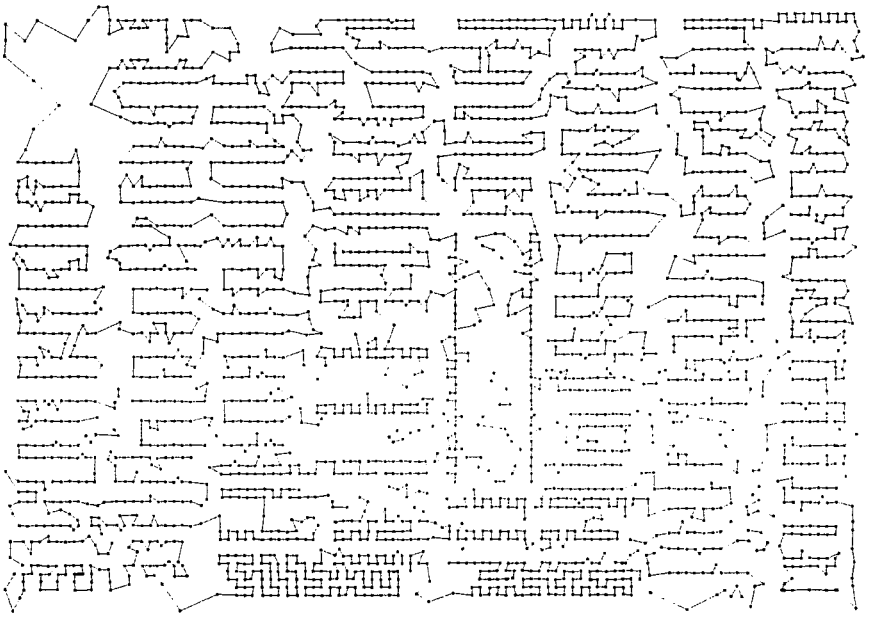
Figuur 9: Kortste route door 13509 plaatsen in Amerika

2. Als Van Gend & Loos pakjes rondbrengt, gebeurt dat vanuit een centraal depot en met meer dan één auto. De planner bepaald eerst welke wagen naar welk adres gaat en lost dan voor elke wagen een handelsreizigers-probleem op; zie figuur 10. In werkelijkheid heb je nog met een heleboel andere factoren te maken: een chauffeur mag maximaal acht uur werken, een klant in een voetgangersgebied moet vóór tien uur 's morgens worden beleverd, de auto staat in een file, enz.



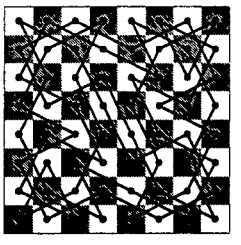
Figuur 10: Routering van drie wagens

3. Een computer bevat vaak rechthoekige platen waarop allerlei onderdelen zijn gemonteerd. Bij de fabricage van zo'n plaat bezoekt een apparaat de talloze montagepuntjes op de plaat om er een druppeltje lijm te deponeren of er met een laserstraal een gaatje in te schieten. Omdat er veel platen moeten worden behandeld, moet het apparaat telkens naar het punt van uitgang terugkeren. Of het nu om lijm of om een laserstraal gaat, het apparaat voert een handelsreizigersroute uit met de montagepuntjes als steden. Dergelijke grote problemen komen in de praktijk vaak voor. In figuur 11 zie je een kortste route voor een probleem met 3038 montage-punten.



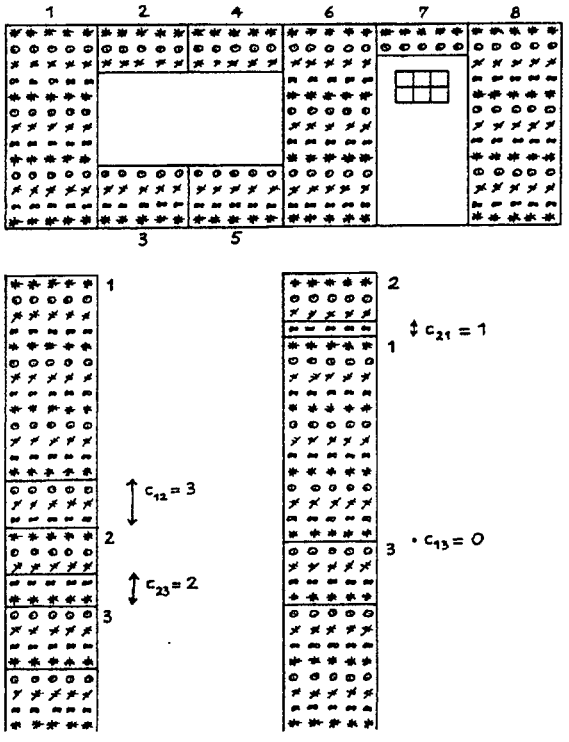
Figuur 11: Kortste route door 3038 montagepunten

4. Is het mogelijk met een paard alle 64 velden van het schaakbord te bezoeken en na 64 zetten op het beginpunt terug te zijn? Dit is een handelsreizigersprobleem met de velden van het schaakbord als steden. De afstand tussen twee steden is het aantal paardensprongen dat nodig is om van het ene veld naar het andere te komen. De vraag is of er een route van lengte 64 is. Het antwoord is ja; zie figuur 12.



Figuur 12: Route van een paard over het schaakbord

5. Je gaat je kamer opnieuw behangen. Je hebt behang uitgezocht met een horizontaal patroon en je wilt dat het patroon over de hele breedte van de muur doorloopt. Twee stukken behang die naast elkaar worden geplakt moeten dus nauwkeurig op elkaar aansluiten. Je wilt de stukken behang nu zodanig uit de rol knippen dat er zo weinig mogelijk verspilling optreedt. De verspilling bestaat uit de stukken behang die je afknipt maar na afloop kunt weggooien. In dit geval zijn de stukken behang die je wilt opplakken de steden. Als je eerst stuk i afknipt en dan stuk j, dan is de lengte van het stuk behang tussen i en j de afstand c_{ij} van i naar j; zie figuur 13. Dit handelsreizigersprobleem is niet helemaal hetzelfde als de andere voorbeelden. In de eerste plaats hoeft de afstand van i naar j niet gelijk te zijn aan die van j naar i. Tot nu toe was dit steeds wel het geval. In de tweede plaats zoek je niet naar een kortste (gesloten) Hamiltoncircuit maar naar een kortste (open) Hamiltonpad. Beide problemen lijken heel veel op elkaar. Als je het circuit-probleem kunt oplossen, kun je het pad-probleem ook aan. Dan laat je immers gewoon de laatste kant weg.



Figuur 13: Het behangen van je kamer

Opmerking

Om de voorbeelden en de opgaven wat eenvoudiger te maken nemen we drie dingen aan:

1. Het handelsreizigersprobleem is een probleem dat wordt beschreven met een **volledige** graaf. M.a.w. tussen elk tweetal steden is er een kant.

2. De afstanden zijn **symmetrisch**, dus $c_{ij} = c_{ji}$ voor elk tweetal steden i, j. We kunnen voor het probleem dus een model maken met een ongerichte graaf. Bij de beschrijving van het probleem hebben we deze veronderstelling eigenlijk al gemaakt. Voorbeelden 1 t/m 5 voldoen aan deze veronderstelling, voorbeeld 6 niet.

3. De afstanden voldoen aan de **driehoeksongelijkheid**, dat wil zeggen: $c_{ik} \leq c_{ij} + c_{jk}$ voor elk drietal steden i, j, k. In woorden: Als je omrijdt schiet je er niets mee op; je legt dan altijd een even lange of langere afstand af dan de rechtstreekse afstand tussen je twee gekozen steden.

Vraag:
Veronderstellingen (2) en (3) betekenen dat $c_{ij} \geq 0$ voor alle ij. De lengtes van de kanten zijn niet-negatief. Kun je dat bewijzen?

4.2 Moeilijkheden van het handelsreizigersprobleem

Het handelsreizigersprobleem kom je zoals je gezien hebt overal tegen: op de weg, in de fabriek en thuis. Het is kenmerkend voor de problemen die we in de **combinatorische optimalisering** tegenkomen:

1. Er worden **discrete** keuzes gemaakt. (Discreet betekent dat je 'ja' of 'nee' kiest, of '0' of '1', 'zwart' of 'wit', er zitten geen grijswaarden tussen. Het probleem is niet continu.) Een kant komt wel of niet in een route voor.

2. Het probleem is makkelijk te omschrijven. Iedereen kan het begrijpen.

3. Maar het probleem is heel lastig optimaal op te lossen.

Nu kun je natuurlijk zeggen: "Hoezo lastig op te lossen?" Veel wiskundigen vinden het juist een heel gemakkelijk probleem. Zij zeggen: "Hoe groot het aantal steden ook is, het aantal mogelijke routes is eindig. Elke route heeft een lengte en onder een eindig aantal routes, die elk een lengte hebben, is er een kortste." Wat ze zeggen is natuurlijk juist; het laat in ieder geval zien dat er een kortste route bestaat. Maar het probleem is die kortste route te vinden, ofwel: het probleem is een **algoritme** te bedenken waarmee je, voor een gegeven probleem, in redelijke tijd een kortste route vindt.

Je zou alle routes één voor één kunnen bekijken, maar dit duurt veel te lang als je veel steden hebt.

Vraag:
Hoeveel routes heb je bij 13 steden?

Als je de bovenstaande vraag hebt kunnen beantwoorden weet je dat er bij 60 steden al meer routes bestaan dan er atomen in het heelal zijn. Toch worden tegenwoordig veel grotere handelsreizigersproblemen snel optimaal opgelost, uiteraard zonder ze allemaal te bekijken.

Wat verstaan we onder snel oplossen? Een algoritme wordt snel genoemd als bij n steden het aantal stappen van de berekening evenredig is met n of n^2 of n-tot-de-een-of-andere constante macht. Een aantal stappen dat evenredig is met 2^n, n^n of $n!$ is traag. Algemeen gesproken noemen we een polynomiale rekentijd redelijk, (uit te drukken in een n-de graads functie, waarbij n een constante is) maar alles wat exponentieel of erger is niet.

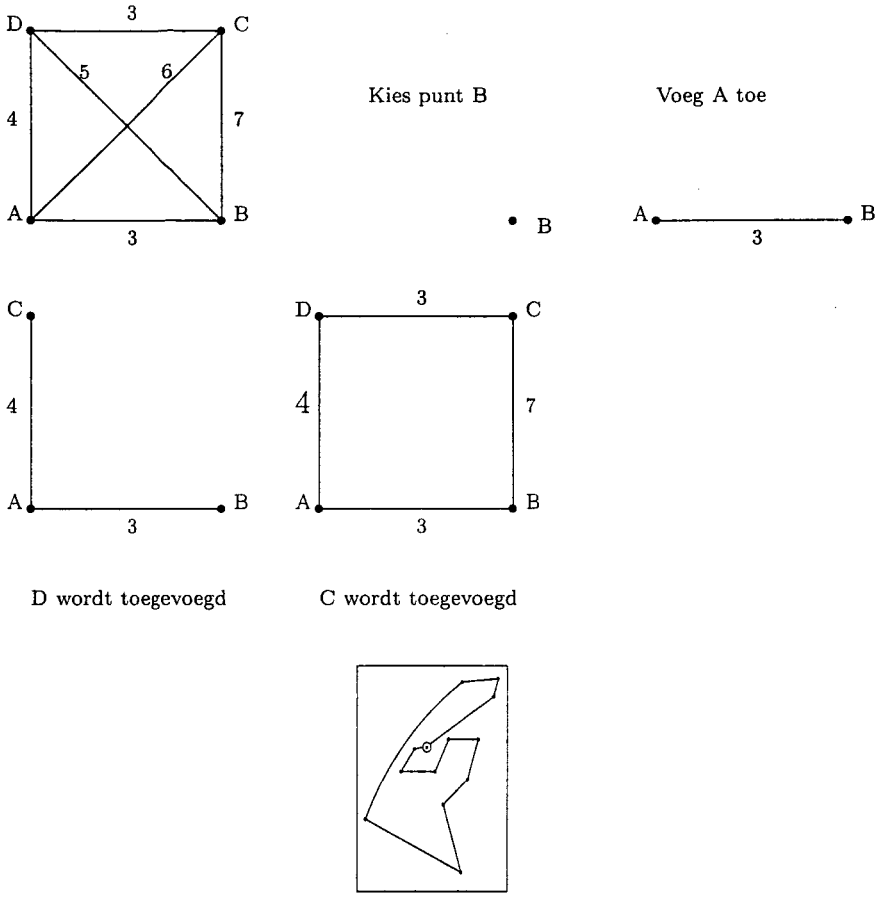
Algoritmes voor het vinden van kortste bomen en kortste paden zijn snel, maar voor het handelsreizigerprobleem bestaat geen snel algoritme dat altijd de snelste route vindt. Tenminste: tot nu toe heeft niemand zo'n algoritme kunnen vinden. Dit betekent dat er keuzes moeten worden gemaakt. Als je echt de kortste route wilt vinden, dan zal dit tijd kosten. Als je die tijd niet hebt, weet je dat je een route vindt die niet per se de kortste hoeft te zijn.

4.3 Algoritmes voor het benaderen van het optimum voor het handelsreizigersprobleem

4.3.1 Het beste-buur-algoritme

Een eenvoudig en snelle regel voor het vinden van een route werkt als volgt:

1. We beginnen in een willekeurige stad.
2. Als je nog niet in alle steden bent geweest dan ga je naar de dichtstbijzijnde nog niet bezochte stad.
3. Als alle steden zijn bezocht, ga dan vanuit de stad waar je bent naar het beginpunt.



Figuur 14: Beste-buur-route vanuit Amsterdam

In figuur 14 zie je hoe dit algoritme het probleem uit voorbeeld 1 heeft opgelost. Het resultaat is helemaal niet optimaal. Een beste-buur-algoritme is meestal matig tot slecht.

4.3.2 Het invoegingsalgortime

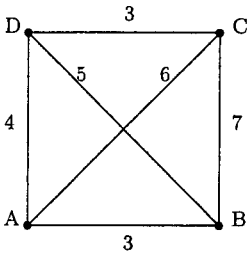
Het beste-buur-algoritme construeert een route door aan een pad telkens een kant toe te voegen. Het invoegingsalgoritme maakt een route door aan een gedeeltelijke route, waar niet alle steden in zitten, steeds een stad toe te voegen. Dit werkt op de volgende manier:

1. Begin met een gedeeltelijke route bestaande uit een willekeurig gekozen stad.

2. Als deze willekeurig gekozen gedeeltelijke route nog niet uit alle steden

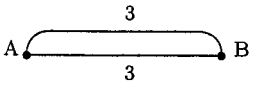
bestaat, kies dan twee steden k en j, met j wel in de route en k niet, zodanig dat c_{jk} minimaal is.

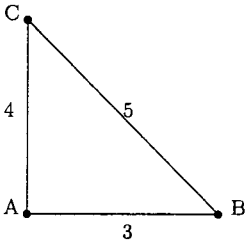
3. Als i een buur van j in de route is, vervang dan de kant ij in de route door ik en kj.



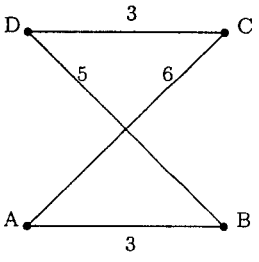
Kies punt B

Voeg A en route AB toe



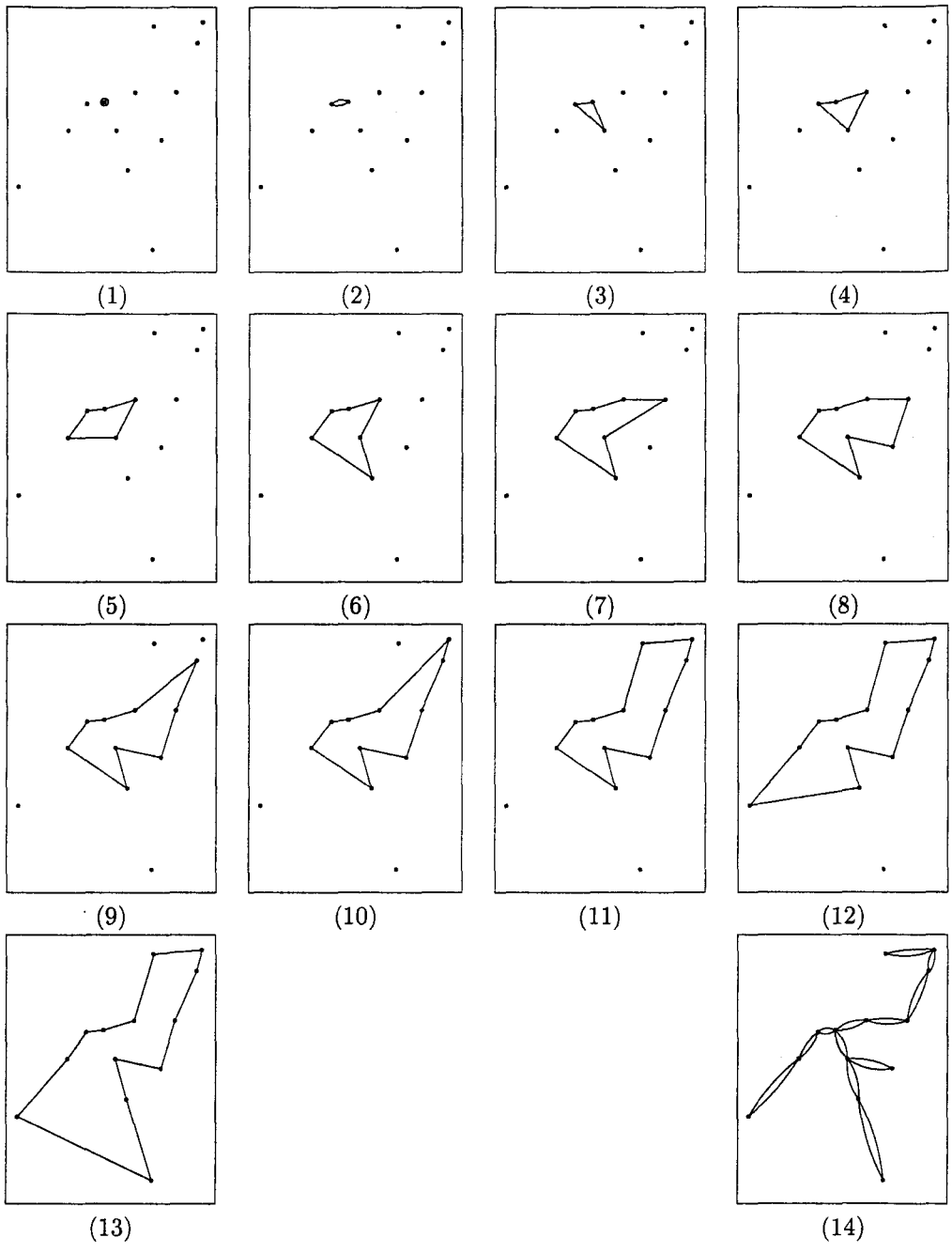


D wordt toegevoegd,
de kanten AD en DB
vervangen AB



C wordt toegevoegd,
de kanten AC en CD
vervangen AD

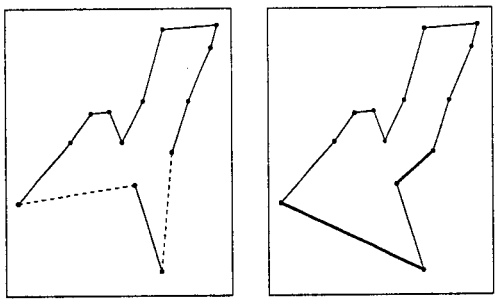
Deze methode lost het probleem uit voorbeeld 1 optimaal op, (zie figuur 14, plaatjes 1 - 13). Het invoegingsalgoritme geeft over het algemeen een beter resultaat dan het beste-buur-algoritme. Er kan nog steeds een groot verschil met het optimum zijn, maar dit verschil blijft begrensd: de route die je met het invoegingsalgoritme vindt is gegarandeerd korter dan twee keer de kortste route.



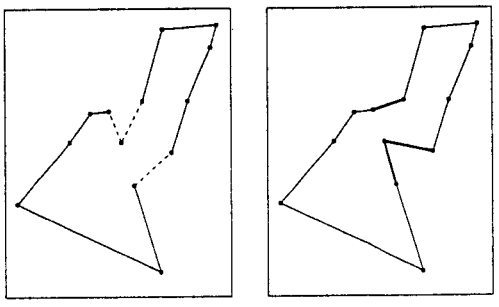
Figuur 15: Het invoegingsalgoritme in actie

4.3.3 Uitwisselingsalgoritmen

Het beste-buur-algoritme en het invoegingsalgoritme construeren stapsgewijs een route. Uitwisselingsalgoritmen gaan uit van een volledige route en proberen die stapsgewijs te verbeteren. Dit gaat meestal via het uitwisselen van kanten. Je kunt natuurlijk zoveel kanten uitwisselen als je zelf zou willen, één, twee of meer. We hebben het dan over 1-uitwisseling, 2-uitwisseling etc. Een t-uitwisseling is dus een uitwisseling waarbij t kanten van een route vervangen worden door t andere kanten, zodanig dat er weer een route ontstaat. Figuur 15 laat een 2-uitwisseling en een 3-uitwisseling zien. Als de nieuwe route korter is dan de oude is er een verbetering bereikt en begint het proces van voren af aan. Dat gaat door totdat de route door een t-uitwisseling niet verder kan worden verbeterd. We noemen de route dan t-**optimaal**.



(a) 2-Uitwisseling



(b) 3-Uitwisseling

Figuur 16: t-Uitwisselingen

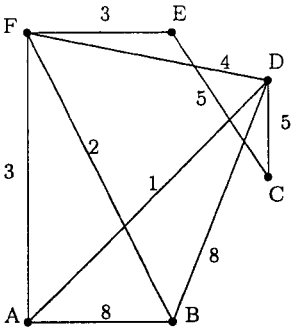
In tegenstelling tot de constructieve algoritmen zijn uitwisselingsalgortimen niet snel. Bovendien kunnen de resultaten net als bij het beste-buur-algoritme behoorlijk slecht zijn, maar dit is dan wel het ergst denkbare geval. In werkelijkheid valt het met de rekentijd en de prestaties erg mee en worden deze algoritmen vaak gebruikt.

4.4 Opgaven

1. Probeer eens een voorbeeld van het beste-buur-algoritme te maken waarvoor het nog slechter gaat dan in figuur 14.

2. Leg uit waarom de route die je met het invoegingsalgoritme vindt korter is dan twee keer de kortste route.

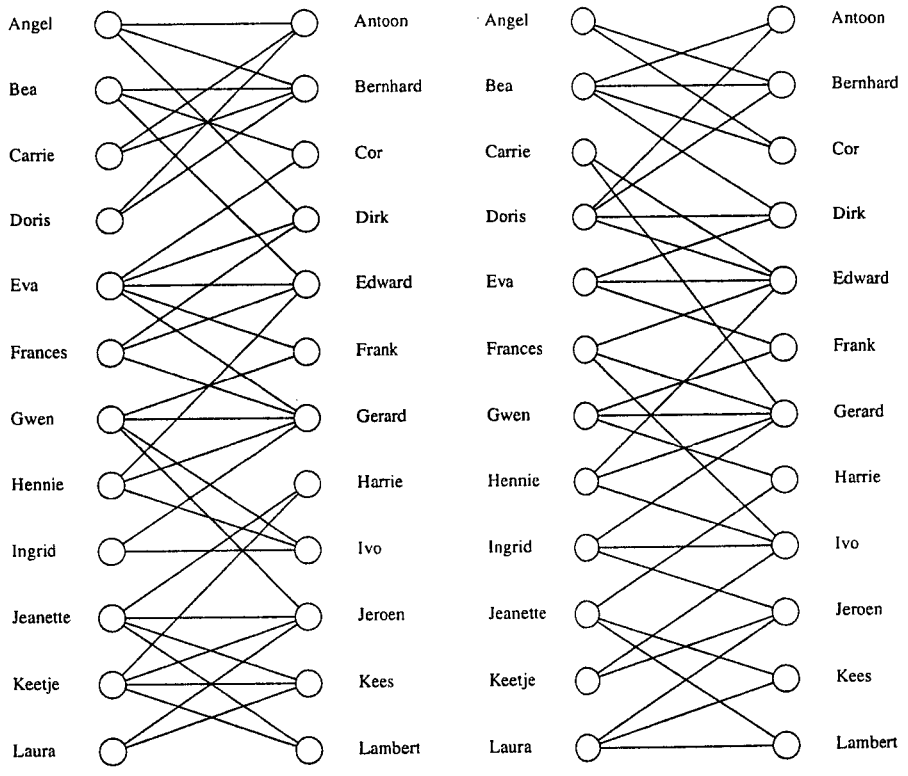
3. Bepaal in onderstaande graaf met alle besproken algoritmes de kortste route tussen $ABCDEF$ N.B. De kanten AE, AC, BC, BE en CF zijn om de graaf overzichtelijk te houden niet getekend. Zij hebben alle lengte 10.



4. Verzin zelf een leuke toepassing bij het handelsreizigerprobleem.

5 Gemengde Opgaven

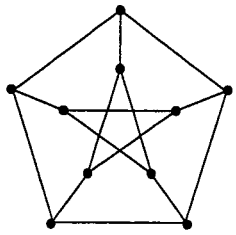
1. Een dansschool heeft als regel dat je je als een stel moet aanmelden, d.w.z.: een jongen en een meisje moeten zich samen aanmelden. Iedereen heeft dan één danspartner. We maken hiervan een voorstelling met een graaf, waarin de punten links de meisjes en de punten rechts de jongens voorstellen. Als een jongen en een meisje mogelijke partners zijn, dan geven we dit aan met een kant tussen de betreffende punten. In figuur 17 zie je twee mogelijke situaties. In die situaties zijn er per persoon ongeveer drie mogelijke danspartners. Zoek voor beide situaties een verdeling in twaalf stellen.



Figuur 17: Problemen rond de dansles

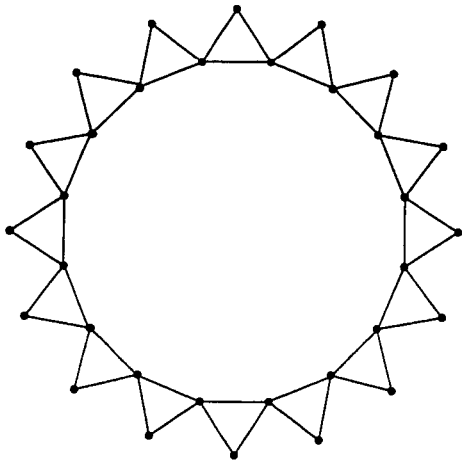
2. In de paragraaf over kortste paden staat in figuur 7 een stukje tekst waarin de mogelijke afbrekingen zijn aangegeven en hoeveel elke afbreking kost. Plaats deze tekst op een bladzijde waarop maar 15 tekens naast elkaar kunnen staan.

3. In figuur 18 zie je de zogenaamde **Petersen**-graaf. Heeft de Petersen-graaf een Hamiltoncircuit?



Figuur 18: Petersen-graaf

4. Het stratenplan in figuur 19 heeft 32 punten. Alle kanten hebben een lengte 1. De afstand tussen twee punten is de lengte van het kortste pad ertussen. Hoe lang is de kortste route langs deze 32 punten? Laat zien dat de beste-buur-algoritme een route zou kunnen vinden (door af en toe een slechte keus te maken wanneer meer dan één adres het dichtstbij ligt) die tweemaal zolang is als de kortste.



Figuur 19: Stratenplan voor 32 adressen

BIJLAGE

Volledige inductie

Volledige inductie is een manier om te bewijzen dat een algoritme, een formule, een patroon voor elk positief geheel getal waar is. Hoe het werkt kun je zien in het volgende voorbeeld:

We tellen steeds opvolgende oneven getallen, beginnend bij 1, bij elkaar op, dus:

$1+3$	$=4$	$=2^2$
$1+3+5$	$=9$	$=3^2$
$1+3+5+7$	$=16$	$=4^2$
$1+3+5+7+9$	$=25$	$=5^2$
$1+3+5+7+9+11$	$=36$	$=6^2$

Het lijkt erop dat de optelling van n opvolgende oneven getallen, beginnend bij 1, steeds n^2 oplevert. Je denkt natuurlijk dat dit altijd zo doorgaat, maar hoe kun je dat bewijzen? We kijken eerst wat we precies willen laten zien. Dat is in dit geval:

$$1+3+5+7+\ldots+(2n-1)=n^2$$

Dit is een bewering en we noemen deze bewering even $P(n)$. Met **volledige inductie** gaan we nu laten zien dat $P(n)$ waar is voor alle mogelijke n. Dit gaat niet door maar willekeurig een heel groot getal in te vullen. Er is namelijk altijd een mogelijkheid dat het voor een nog groter getal niet meer geldt en het is natuurlijk onmogelijk om alle getallen te controleren. Eigenlijk hebben we maar twee dingen nodig. Eerst moeten we laten zien dat $P(n)$ waar is voor $n=1$ (dat wil zeggen $P(1)$ is waar) en dan willen we laten zien dat als $P(n)$ waar is voor een willekeurige n, dat dan automatisch $P(n+1)$ ook waar is. Je kunt je dit misschien voorstellen als een soort domino-effect. Als één dominosteen valt dan valt de volgende ook en die daarna ook en die daarna, enzovoorts. Dus als we de allereerste steen omgooien (als $P(1)$ waar is), dan valt de hele rij dominostenen ($P(n)$ is dan waar voor alle n), omdat elke steen door zijn voorganger zal worden omgetikt, en zelf weer zijn opvolger omgooit.

Dus in ons geval kijken we eerst of geldt:

$$1=1^2$$

Dit is natuurlijk flauw. Laten we nu eens aannemen dan $P(n)$ waar is voor een willekeurige n. Dus neem aan dat:

$$1+3+5+7+\ldots+(2n-1)=n^2$$

Het volgende oneven getal na $(2n-1)$ is $(2n+1)$. We tellen dit bij allebei de kanten van het gelijkteken in onze bewering op:

$$1 + 3 + 5 + 7 + \ldots + (2n - 1) + (2n + 1) = n^2 + (2n + 1)$$

We weten dat $(n + 1)^2 = n^2 + 2n + 1$, dus wordt het voorgaande nu:

$$1 + 3 + 5 + 7 + \ldots + (2n - 1) + (2n + 1) = (n + 1)^2$$

en dat is precies $P(n + 1)$. We hebben dus laten zien dat *als* $P(n)$ waar is voor een willekeurige n *dan* is ook $P(n + 1)$ waar.

We hadden n willekeurig gekozen en daarom mogen we nu ook elk geheel getal dat we kunnen bedenken invullen. Als ik $n = 1$ neem dan is $P(1)$ waar, dat was duidelijk. Je ziet uit het voorgaande dat dan $P(2)$ ook waar is. Maar als $P(2)$ waar is, dan is ook $P(3)$ waar, enz. De bewering zal altijd gelden dus hebben we met behulp van volledige inductie kunnen vaststellen dat $P(n)$ inderdaad voor alle positieve gehele getallen n waar is.

Literatuurlijst

- "Graphs, An Introductory Approach" - *Robin J. Wilson and John J. Watkins.*

Docentenhandleiding

"Kun je me de kortste weg vertellen?"

Technische Universiteit Eindhoven
M.M.C. Tuyp
April 2002

Inleiding

Het boekje 'Kun je me de kortste weg vertellen?' is een bewerking van de masterclass combinatorische optimalisering gegeven op 5 maart 1999 door Prof. Dr. J.K. Lenstra in samenwerking met Dr. Ir. C. Hurkens. De bewerking is gemaakt door Mw. M.M.C. Tuyp, student wiskunde aan de TU/e en docent wiskunde aan B.C. Broekhin te Roermond.

Het onderwerp 'Optimaliseren' met behulp van grafen wordt in het VO nauwelijks behandeld. De eerste keer dat leerlingen met grafen in aanraking komen is in een oppervlakkig hoofdstukje in de brugklas. Daarna in klas drie en vervolgens komt het onderdeel even aan de orde bij 'Grafen en Matrices' in 5VWO wiskunde A1 en A1,2. In de jaren 2002 en 2003 is 'Grafen en Matrices' geen onderdeel van het Centraal Examen A1 en A1,2 en staat het de docenten vrij om hierover vragen te stellen in de schoolexamens voor wiskunde A1 en A1,2. Voor de wiskunde B1 en B1,2 leerlingen komt het onderwerp na leerjaar 3 niet meer aan de orde.

De reader 'Kun je me de kortste weg vertellen?' verteld over modelleren en het oplossen van optimalisatieproblemen met behulp van grafen. Het materiaal is geschikt om te lezen, enige opgaven te maken en zelf aan de hand van suggesties die in het boekje worden gegeven enig onderzoek te doen.

Doel

Het is niet de bedoeling dat de leerlingen (of een docent) het doorwerken van het boekje zien als een profielwerkstuk op zich. Het is meer bedoeld als diepgaande informatiebron, een instap voor het onderzoeksonderwerp. Na het doorwerken van het boekje is het de bedoeling dat de leerlingen in ieder geval de volgende vaardigheden enigzins onder de knie hebben:

- Een leerling kan een simpel probleem vertalen naar een model.
- Een leerling kan een 'kortste boom' probleem oplossen.
- Een leerling kan een 'kortste pad' probleem oplossen.
- Een leerling kent enige algoritmes voor het benaderen van het optimum voor het handelsreizigersprobleem.
- Een leerling weet dat de optimale oplossing bij het benaderen van het optimum voor het handelsreizigersprobleem niet altijd kan worden gevonden en kan in eigen bewoordingen uitleggen waarom dit is.

Met deze vaardigheden zou de leerling op zoek kunnen gaan naar een probleem of puzzel. Hij/zij zou in een bibliotheek of op het internet op zoek kunnen gaan en zijn/haar bevindingen kunnen verwerken in een profielwerkstuk. Uiteraard kan het materiaal uit de reader en eventueel uitgewerkte opgaven als informatie worden bijgevoegd. Op de volgende sites kunnen interessante informatie en ideëen gevonden worden.

http://archives.math.utk.edu/liberal.arts/gt2.html
http://www.maa.org/mathland/mathtrek_2_8_99.html
http://www.c3.lanl.gov/mega-math/workbk/graph/grbkgd.html

Doelgroep en vereiste voorkennis

Dit onderwerp is geschikt voor leerlingen uit de klassen 5 en 6 VWO met profiel N&G of N&T. Speciale voorkennis is niet vereist.

Tijdsduur

De tijdsduur van het doornemen van het boekje zal afhangen van het aantal gemaakte opgaves. Een minimum van 16 uur kan wel worden aangenomen.

Benodigde materialen

Computer en/of GR. Er zijn veel leuke pagina's te vinden op het internet die met behulp van JAVA-applets bewerkingen op grafen uitvoeren. Op de site http://math.exeter.edu/rparris/ staan een negental freewareprogrammaatjes, waaronder het programmaatje windisc waarmee hele aardige bewerkingen op grafen kunnen worden uitgevoerd.

Gewenste begeleiding

In theorie is het boekje 'Kun je de kortste weg vertellen?' zo opgebouwd dat de leerling met zelfstudie en het maken van de opgaven alsmede wat onderzoek op het internet geen extra begeleiding nodig heeft.

Kun je me de kortste weg vertellen?

Inhoudsopgave

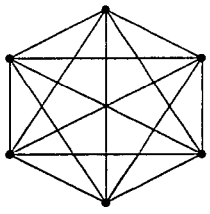
Combinatorische Optimalisering
Uitwerkingen

28 november 2000

1 Grafen

1.2

1. *
2. *
3. (a) De volledige graaf met 6 punten:



   (b) $\frac{1}{2}n(n-1)$
4. A, B en D zijn gelijk.

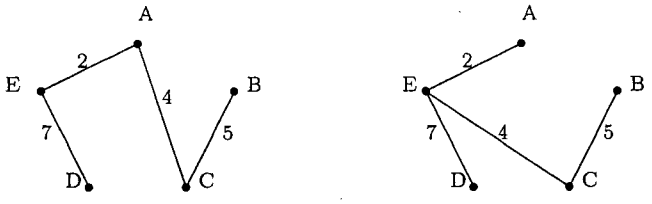
2 Kortste bomen

Vraag:
Waarom kan een kortste boom geen circuits hebben? (pag. 5)

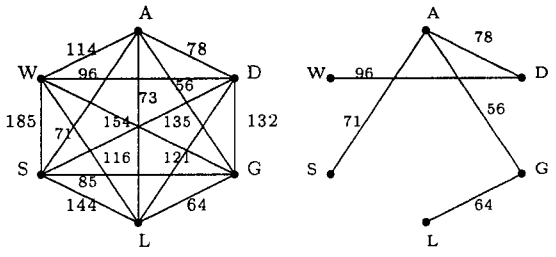
Antwoord:
Als er een circuit zou bestaan, dan kun je één van zijn kanten weglaten. Dat bespaart kosten en alle punten blijven nog steeds met elkaar verbonden.

2.3

1. Er zijn maar twee kortste bomen.



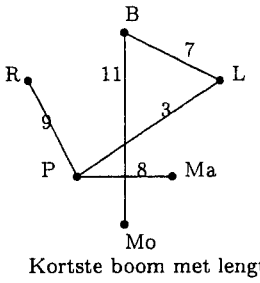
2. Graaf en bijbehorende kortste boom met lengte 365:



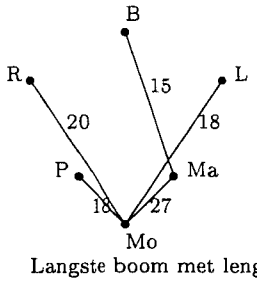
3. De inbreker maakt bij de graaf een kortste opspannende boom. Alle kanten die niet in de boom zitten kan hij weghalen.

4. Kies nu in het algoritme in plaats van steeds een kant met minimale lengte de kant met maximale lengte.

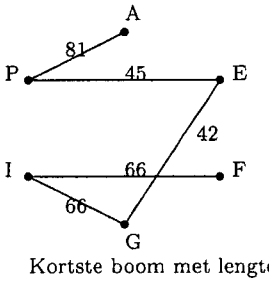
5. Kortste en langste opspannende bomen.



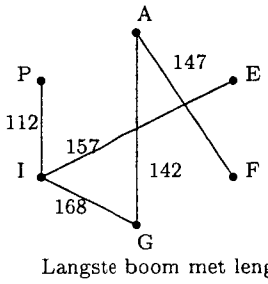
Kortste boom met lengte 38



Langste boom met lengte 88



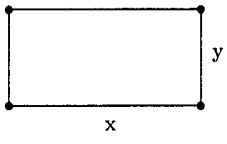
Kortste boom met lengte 300

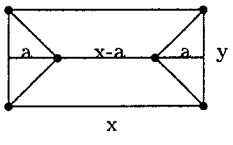


Langste boom met lengte 726

2.5

1. Zie uitwerkingen 2.3.
2. $x = \frac{1}{3}\sqrt{3}$ dus de lengte van de Steiner-boom is $\sqrt{3}$
3. Bij een rechthoekige graaf op 4 punten met lengte x en breedte y geldt dat de punten die worden toegevoegd om de Steiner-boom te vormen, liggen op een afstand $\frac{1}{2}y$ van de langste zijden en een afstand $a = \frac{y}{2\sqrt{3}}$ van de kortste zijden.





3 Kortste paden

3.2

1. Het kortste pad van S naar T is $SABDT$ met lengte 22.
2. $AB = BA = 35$, $AC = CA = 35$, $AD = DA = 25$, $AE = EA = 10$,
   $BC = CB = 20$, $BD = DB = 30$, $BE = EB = 25$,
   $CD = DC = 10$, $CE = EC = 25$,
   $DE = ED = 35$.

3. De kortste routes zijn: $SA = 1$, $SB = 3$, $SC = 5$, $SD = 3$, $SE = 4$, $SF = 6$, $ST = 8$.

4. Nee, dit kan niet. De graaf is niet gericht. Je kunt eindeloos in cirkels rondlopen en de routes zo steeds langer maken.

5. De eerste lengte $L(1) = 0$ is natuurlijk goed. Stel nu eens dat alle lengtes tot een bepaald punt n goed zijn. We voeren stap 2 van het algoritme uit om het volgende punt k aan ons kortste pad toe te voegen. Voor dit punt moet gelden $M(k) > L(n) + c_{nk}$ zodat we $M(k) = L(n) + c_{nk}$ hebben uitgevoerd. We kiezen het $(n+1)^{ste}$ punt uit de punten k die nog geen lengte hebben zodanig dat $M(n+1) \leq M(k)$ voor alle k. Hierdoor garanderen we dat alle lengtes tot het punt $(n+1)$ goed zijn. We kunnen nu zeggen dat de juistheid van het kortste pad tot het punt $(n+1)$ volgt uit het kortste pad tot het punt n en omdat we n willekeurig kunnen kiezen, geldt die voor àlle n en dus ook voor alle punten van de graaf als we n gelijk stellen aan het aantal punten van de graaf.

4 Kortste routes

4.1 Handelsreizigers

Vraag:
Veronderstellingen (2) en (3) betekenen dat $c_{ij} \geq 0$ voor alle ij. De lengtes van de kanten zijn niet-negatief. Kun je dat bewijzen? (pag. 29)

Antwoord:
Volgens (3) geldt $c_{ik} \leq c_{ij} + c_{jk}$ voor elk drietal steden i, j, k, dus ook $c_{ij} \leq c_{ik} + c_{jk}$ en volgens (2) geldt $c_{jk} = c_{kj}$, dus $c_{ij} \leq c_{ik} + c_{kj}$.

Stel nu dat $c_{jk} = c_{kj} < 0$, dan geldt ook $c_{ik} \leq c_{ij}$ en $c_{ij} \leq c_{ik}$. Hieruit volgt dat $c_{ij} = c_{ik}$, dus moet wel gelden $c_{jk} = c_{kj} = 0$. Dit is in tegenspraak met de aanname dat $c_{jk} = c_{kj} < 0$.

4.2 Moeilijkheden van het handelsreizigersprobleem

Vraag:
Hoeveel routes heb je bij 13 steden? (pag. 30)

Antwoord:
$\frac{1}{2}(13-1)! = 239.500.800$

4.4

1. *

2. Het algoritme voegt een stad k in door een kant ij te vervangen door twee kanten ik en kj. Zo'n vervanging kun je zien als twee stappen:

   (a) Eerst wordt er een dubbele kant kj toegevoegd.

   (b) Dan worden de kant ij en één van de kopieën van kant kj vervangen door de kant ik.

   Als je alleen de stap (a) uitvoert en stap (b) achterwege laat, krijg je een dubbele kortste boom. Dat komt omdat je k en j zodanig kiest dat c_{jk} minimaal is. Nu is een kortste boom korter dan een kortste route, want als je uit een kortste route een kant weglaat krijg je een boom en de kortste boom kan niet langer zijn dan die boom. De dubbele kortste boom is dus korter dan twee keer de kortste route.

   Stap (b) maakt uit de dubbele boom een route door telkens twee kanten door één kant te vervangen. De driehoeksongelijkheid zegt dat de nieuwe kant niet langer is dan de twee oude samen. De route die zo ontstaat is dus niet langer dan de dubbele boom en dus korter dan twee keer de kortste route.

3. Beginnend in F vind je met het BB-algoritme lengte 32.
   Beginnend in F vind je met het IV-algoritme lengte 32.

4. *

5 Gemengde Opgaven

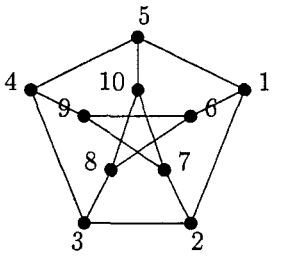
1. Een mogelijke verdeling in 12 stellen voor Situatie 1. is:

Angel	- Dirk
Bea	- Cor
Carrie	- Antoon
Doris	- Bernhard
Eva	- Frank
Frances	- Gerard
Gwen	- Jeroen
Hennie	- Edward
Ingrid	- Ivo
Jeanette	- Harrie
Keetje	- Lambert
Laura	- Kees

   Voor Situatie 2. bestaat geen verdeling, want Carrie, Frances, Hennie, Ingrid en Keetje willen alleen samen met Edward, Gerard, Ivo en Jeroen. Er blijft dan één meisje zonder partner.

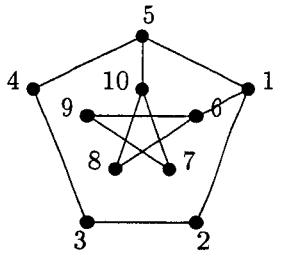
2. Deze tekst kan
op dertig
plaatsen worden
afgebroken.
Sommige
afbrekingen
zijn lelijker
dan andere.

3. Nee, de Petersen-graaf heeft geen Hamiltoncircuit.



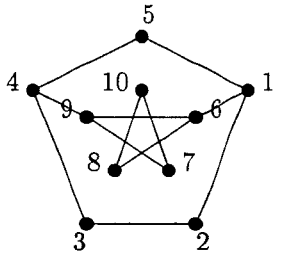
Als er een Hamiltoncircuit zou bestaan, dan moet er tenminste een kant zijn die begint in het buitenste pentagon en eindigt in de binnenste ster. De Petersen-graaf is symmetrisch, dus je kunt willekeurig één van de 5 kanten nemen die hieraan voldoet. Neem maar eens kant (1,6). Verder kunnen we ook concluderen dat het aantal kanten dat de ster met het pentagon in een Hamiltoncircuit verbindt even moet zijn, je moet immers terug naar je beginpunt. Daarvan zijn twee mogelijke gevallen denkbaar, een met twee kanten tussen de ster en het pentagon en een met 4 kanten tussen de ster en het pentagon.
Weer omdat de Petersen-graaf symmetrisch is, voldoet het voor het geval met twee kanten tussen de ster en het pentagon als je kijkt naar het geval (a) waarin de kanten (1,6) en (5,10) voorkomen en het geval (b)waarin de kanten (1,6) en (4,9) voorkomen. Voor het geval met de 4 kanten tussen de ster en het pentagon is het voldoende als je kijkt naar het geval (c) waarin de kanten (1,6), (5,10), (4,9) en (3,8) voorkomen.

(a) Teken eerst de graaf waarin je de kanten die je niet nodig hebt weg laat.



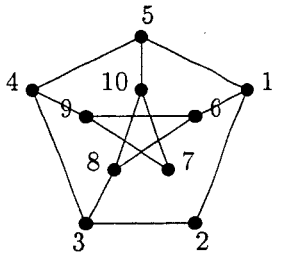
Er is in dit geval geen pad van knoop 6 naar knoop 10 dat alle knopen van de ster bevat, dus het is niet mogelijk hier een Hamiltoncircuit van te maken.

(b) Teken nu de Petersen-graaf zonder de kanten (5,10), (3,8) en (2,7).

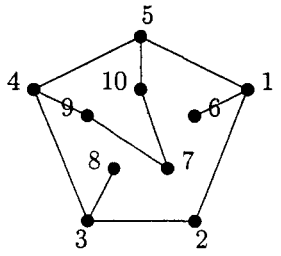


Ook hier kun je geen Hamiltoncircuit van maken omdat het nu niet mogelijk is om alle punten van het Pentagon langs te gaan.

(c) De enige mogelijkheid die je over hebt is de graaf waar je even de kant (2,7) uit weg laat.



Knoop 7 moet in het circuit zitten dus ben je gedwongen de kanten (10,7) en (7,9) in je circuit toe te voegen. Knoop 2 moet ook in je circuit zitten dus voeg je de kanten (1,2) en (2,3) toe. Je hebt dan het volgende:



Nu zit je vast, want knoop 8 moet graad 2 hebben binnen het circuit. Kant (8,10) kun je niet toevoegen want dan heeft knoop 10 graad 3. Kant (8,6) kun je ook niet toevoegen want dat geeft een subcircuit en dat kan niet binnen een Hamiltoncircuit. Met andere woorden de Petersen-graaf heeft geen Hamiltoncircuit.

4. De kortste route is 32.