Inleiding

God schiep de natuurlijke getallen, de rest is het werk van de mens — Kronecker

Discreet versus numeriek

De *natuurlijke getallen* hebben hun naam niet gestolen. Ze staan voor het meest (be)grijpbare begrip uit de getallenwereld — menig kleuterversje parafraseert dan ook het rijtje dat steevast begint met "1 2 3 ...". Pas in een later stadium komen de begrippen nul, negatieve getallen, breuken, niet-rationale getallen aan bod. Totdat op het einde van de middelbare school de natuurlijke getallen helemaal op de achtergrond verdwenen zijn. Ten voordele van de analyse van continue krommen met domein en beeld in $\mathbb{R}$, de analytische meetkunde met oneindig veel punten op een rechte (die dan 'oneindig dicht' bij elkaar liggen) enzovoort. De ideale wiskundige achtergrond om Newtoniaanse fysica mee te bedrijven.

Aan het begin van je hogere studies (cfr foutberekeningen in labo's fysica), blijkt dan dat er toch wat problemen opduiken bij de wiskunde die gebruik maakt van reële getallen. Of niet zozeer met de wiskunde zelf, dan wel met de wijze waarop we exacte resultaten uit de theorie willen halen. Willen we berekeningen zeer nauwkeurig en snel uitvoeren (om te beginnen zonder logaritmetafels), dan moeten we beroep doen op computers. Maar zelfs de krachtigste computers hebben hun fysieke beperkingen... en laten dus geregeld een steekje (lees: een deel achter de komma) vallen. Om de problemen die hieruit voortkomen te onderkennen en op te vangen (afrondingsfouten, schijnbaar niet-convergerende berekeningen,...) maakt men gebruik van wiskundige methodes en theorieën die men onderbrengt onder de noemer *numerieke wiskunde*. Deze tak van de wiskunde houdt zich dus bezig met de discrepantie tussen de gewenste reële uitkomsten, en de gebruikte berekeningsmethodes die beperkt zijn in hun voorstellingsvermogen.

Laten we nu even de gekende toepassingsgebieden van de computer als krachtige rekenmachine buiten beschouwing, en kijken we alleen naar de machine zelf. Het staat buiten kijf dat de inwendige werking van een digitale computer een uitgesproken discreet karakter heeft: een bit heeft de waarde 0 dan wel 1, maar niets daartussen. Dit impliceert dat analyseren en logisch redeneren zoals dat in informatica-context voorkomt, ook een uitgesproken discreet karakter zal hebben. De deeltak van de wiskunde die zich ontfermt over alle methodes en theorieën met een *discrete* invalshoek, wordt de *discrete wiskunde* genoemd.

Wij zullen ons in deze cursus bezighouden met enkele elementaire begrippen en theorieën uit de discrete wiskunde — maar weet dat er nog veel meer rond te vertellen, onderzoeken en ontdekken valt (ook nú nog, de grote ontdekkingsreizigers van de wiskunde dateren niet allemaal uit de Griekse tijd of de Verlichting).

Om ons in genoeg houvast en links met de realiteit te voorzien, hieronder enkele toepassingsgebieden van de theorie(en) die de discrete wiskunde ons aanreikt.

- fysica
- chemie
- biologie
- communicatie
- elektronica en elektriciteit
- cryptografie
- codeertheorie
- akoestiek
- muziek
- informatica
  - computerarchitectuur en hardware design
  - design van softwaresystemen
  - beveiliging
  - generatie van random getallen
  - digitale signaalverwerking
  - computergrafiek en beeldverwerking
  - foutopsporing en -verbetering
  - analyse en design van algoritmen

Keer op het einde van de cursus nog eens terug naar dit lijstje, om na te gaan welke toepassingsgebieden van de discrete wiskunde we aanraakten in deze nota's.

God schiep de getallen 0 en 1, de rest is het werk van de computer — parafrasering van Kronecker door informatici

Grieks alfabet

A	α	alpha	___	N	ν	nu	___
B	β	beta	___	Ξ	ξ	xi	___
Γ	γ	gamma	___	O	o	omikron	___
Δ	δ	delta	___	Π	π	pi	___
E	ϵ	epsilon	___	P	ρ	rho	___
Z	ζ	zèta	___	Σ	$\sigma\ \varsigma$	sigma	_____
H	η	èta	___	T	τ	tau	___
Θ	θ	thèta	___	U	υ	upsilon	___
I	ι	iota	___	Φ	$\varphi\ \phi$	phi	_____
K	κ	kappa	___	X	χ	chi	___
L	λ	lambda	___	Ψ	ψ	psi	___
M	μ	mu	___	Ω	ω	omega	___

Romeinse getallen

I	1
V	5
X	10
L	50
C	100
D	500
M	1000

Hoofdstuk 1

Basisbegrippen

In dit hoofdstuk gaan we eerst na wélke soorten getalsystemen er bestaan en hoe we die getallen dan best noteren. Uiteraard zullen voornamelijk de discrete en de eindige systemen ($\mathbb{N}$ en $\mathbb{Z}/_{n\mathbb{Z}}$) van belang zijn voor het vervolg van de cursus. Meteen wordt ook een belangrijke toepassing van $\mathbb{N}$ aangehaald: het principe van inductie (zowel de wiskundige bewijsmethode die inductie gebruikt, als recursieve definities, formules en functies die geregeld in wiskundig getinte programma's opduiken).

Er komen al een aantal bewijzen voor in dit hoofdstuk. Op het einde van hoofdstuk 2 delen we bewijzen in naargelang de redenering die gebruikt werd (bewijs met inductie, bewijs uit het ongerijmde, gevallenstudie,...). Keer nadien dus terug naar dit hoofdstuk, om na te gaan of je de (deel-)bewijzen kan classificeren volgens bewijsmethode.

1.1 Getallenverzamelingen

1.1.1 De natuurlijke getallen

$$\begin{array}{lcl} \mathbb{N} & = & \{0, 1, 2, 3, ...\} \\ \mathbb{N}_0 & = & \{1, 2, 3, ...\} \end{array}$$

Of nul al dan niet een natuurlijk getal genoemd wordt, is enkel een kwestie van definitie (lees: afspraak). Het is echter een feit dat het getal 0 pas lang na de andere getallen zijn intrede deed. En gelukkig maar dát het er is, anders telden we nog op zoals de Romeinen: uit 5+5=10 volgt makkelijk dat 50+50=100, maar uit V+V=X leid je niet zo makkelijk af dat L+L=C.

Eigenschappen van $\mathbb{N}$

- gesloten onder $+$ en $\times$ (als $a, b \in \mathbb{N}$, dan ook $a + b \in \mathbb{N}$ en $a \times b \in \mathbb{N}$)
- niet gesloten onder $-$ (uitbreiding tot $\boldsymbol{Z}$ nodig)
- niet gesloten onder $/$ (uitbreiding tot $\mathbb{Q}$ nodig)
- heeft natuurlijke ordening $<$
- getallen van $\mathbb{N}$ zijn ideale '*tellers*': ze vormen de natuurlijkste/eenvoudigste labels om een telling uit te voeren. Ze vormen uiteraard niet de enige mogelijkheid. Doch élk telproces gebruikt labels waarvan het patroon overeenkomt met dat van $\mathbb{N}$: je start met een eerste element, en voor elk element is er een uniek volgend element. Ga maar na: zelfs al tel je per 100 beginnend vanaf 50, dan heb je nog een eenvoudige overeenkomst tussen je zelfgekozen labels en $\mathbb{N}$ of $\mathbb{N}_0$:

50	150	250	350	450	...
↓	↓	↓	↓	↓	
1	2	3	4	...	

- elk getal uit $\mathbb{N}$ heeft dus een opvolger, en elk getal m van $\mathbb{N}$ kan uit 0 bekomen worden door (een eindig aantal) opeenvolgende opvolgers te beschouwen. Dit sluit zeer nauw aan bij iteratie of recursie en maakt meteen duidelijk dat $\mathbb{N}$ door een informaticus niet overschat kan worden.

1.1.2 De gehele getallen

$$\boxed{\boldsymbol{Z} = \{..., -2, -1, 0, 1, 2, ...\}}$$

De $\boldsymbol{Z}$ staat voor *Zahlen*, Duits voor *getallen*.

Voordelen ten opzichte van $\mathbb{N}$

- $\boldsymbol{Z}$ is een **ring**: gesloten voor $+, \times$ én $-$. Zie bijlage D.
- met minimale uitbreiding van $\mathbb{N}$ (nl. één extra element per element verschillend van nul), zijn de kansen om een wiskundige berekening te kunnen uitvoeren, merkbaar verhoogd.

Nadeel ten opzichte van $\mathbb{N}$

- cruciale inductie-eigenschap van $\mathbb{N}$ is verloren gegaan. Het is nu onmogelijk om bij een willekeurig element van $\boldsymbol{Z}$ uit te komen als je start bij een *vast gegeven geheel getal*, en enkel opvolgers mag nemen.

1.1.3 De rationale getallen

$$\boxed{\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\}}$$

Voordeel ten opzichte van $\mathbb{Z}$

- $\mathbb{Q}$ is een **veld**: gesloten voor $+, \times, -$ én $/$.

Nadeel ten opzichte van $\mathbb{Z}$

- discrete ordening gaat verloren: je kan voor een rationaal getal niet aangeven wat zijn (unieke) opvolger is. Tussen elke twee rationale getallen x en y ligt namelijk een ander: $\frac{x+y}{2}$. De ordening is *dicht*.

1.1.4 De reële getallen

De reële getallenverzameling $\mathbb{R}$ kan niet zo eenvoudig omschreven worden als de vorige verzamelingen, tenzij we een meetkundige interpretatie aanhalen: de reële getallen stellen alle punten op een (geijkte) lijn voor; de reële getallenas. Hoewel de rationale getallen reeds dicht op elkaar zitten op die getallenas, zijn er altijd nog lengtes die we wel kunnen waarnemen, maar die niet overeenkomen met rationale getallen. Twee voorbeelden: $\sqrt{2}$ en π (de diagonaallengte van een vierkant met zijde 1, resp. de omtrek van een cirkel met diameter 1).

Stelling 1.1. *Het getal $\sqrt{2}$ is niet rationaal.*

Bewijs Dit wordt een bewijs uit het ongerijmde (zie blz 42). We onderstellen dat $\sqrt{2} \in \mathbb{Q}$, en komen (na enig logisch redeneerwerk) uit op een contradictie. Daaruit valt (gezien het waterdichte redeneerwerk) uit te concluderen dat de premisse (de vooropgestelde onderstelling) fout is.

Stel $\sqrt{2} \in \mathbb{Q}$. Dus $\sqrt{2} = \frac{a}{b}$, met $a \in \mathbb{Z}$ en $b \in \mathbb{N}_0$. We kiezen a en b zó dat a en b onderling ondeelbaar zijn.[1] (Dus $\text{ggd}(a, b) = 1$; indien dit niet het geval was, stel $ggd(a, b) = c$, dan

[1] Twee getallen zijn onderling ondeelbaar als hun grootste gemene deler (ggd) gelijk is aan 1. Zie blz 71.

vervangen we a door $\frac{a}{c}$ en b door $\frac{b}{c}$.)

$\sqrt{2} = \frac{a}{b}$	
$\Rightarrow \quad 2 = \frac{a^2}{b^2}$	
$\Rightarrow \quad 2b^2 = a^2$	
$\overset{(1)}{\Rightarrow} \quad a^2$ is even	(1) : $b \in \mathbb{N}$
$\overset{(2)}{\Rightarrow} \quad a$ is even	(2) : kwadraat van oneven getal is oneven
$\Rightarrow \quad a = 2c$, voor zekere $c \in \mathbb{Z}$	
$\Rightarrow \quad a^2 = 4c^2$	
$\Rightarrow \quad 4c^2 = 2b^2$	
$\Rightarrow \quad 2c^2 = b^2$	
$\overset{(3)}{\Rightarrow} \quad b$ is even	(3) : analoge redenering als bij a

Dit is een contraditie: als a en b beide even zijn (zoals hierboven aangetoond), is $\text{ggd}(a, b) \neq 1$. Dus is de oorspronkelijke onderstelling verkeerd, en $\sqrt{2} \notin \mathbb{Q}$. □

Voordeel ten opzichte van $\mathbb{Q}$

- Reële getallen spelen een cruciale rol in de ontwikkeling van de wiskundige analyse, en stemmen overeen met de natuurlijke intuïtie. (Denk maar aan de middelwaardestelling: niet mogelijk als er gaten in je getallenas zitten!)

1.1.5 Complexe getallen

$$\boxed{\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}}$$

Voordeel ten opzichte van $\mathbb{R}$

- Alle veeltermvergelijkingen in één onbekende kunnen nu opgelost worden (om te beginnen de vergelijking $x^2 + 1 = 0$). Zelfs de veeltermvergelijkingen met complexe coëfficiënten: $\mathbb{C}$ is een algebraïsch gesloten veld.

Nadeel ten opzichte van $\mathbb{R}$

- Getallen zijn niet meer op een natuurlijke manier te ordenen, maar het best gevisualiseerd in het vlak.

1.2 Modulorekenen

Tot nu toe herhaalden we de meest bekende getalsystemen (verzamelingen van getallen met bijhorende bewerkingen die altijd kunnen uitgevoerd worden in die verzameling). We zetten ze even op een rijtje:

$\mathbb{N}$	gesloten onder	$+$	$\times$			
$\mathbb{Z}$	gesloten onder	$+$	$\times$	$-$		
$\mathbb{Q}$	gesloten onder	$+$	$\times$	$-$	$/$	
$\mathbb{R}$	gesloten onder	$+$	$\times$	$-$	$/$	
$\mathbb{C}$	gesloten onder	$+$	$\times$	$-$	$/$	en algebraïsch gesloten (alle veeltermen in x hebben oplossing)

Er zijn echter nóg interessante getalsystemen.Veruit de meest interessante in de discrete wiskunde (en dus voor informatici) heb je al wel gebruikt, maar ben je misschien nog niet formeel tegengekomen. Het gaat om de eindige verzamelingen $\mathbb{Z}/_{n\mathbb{Z}}$ (de gehele getallen modulo n), met bijhorende optellings- en vermenigvuldigingsoperatoren.

$$\boxed{\mathbb{Z}/_{n\mathbb{Z}} = \{0, 1, 2, \ldots, n-1\}, \quad n \in \mathbb{N}, n \geq 2}$$

Deze $+$ en $\times$ zijn echter niet dezelfde als de $+$ en $\times$ op gehele getallen: we willen immers dat $\mathbb{Z}/_{n\mathbb{Z}}$ gesloten is onder deze operatoren. Volgende definitie van $+$ en $\times$ in $\mathbb{Z}/_{n\mathbb{Z}}$ voldoet aan deze voorwaarde:

> *Optellen respectievelijk vermenigvuldigen gebeurt eerst zoals in $\mathbb{Z}$, waarna die (tussen-)uitkomst wordt vervangen door zijn rest bij deling door n.*

Opgelet! Als je de modulo-operator gebruikt in programmacode, ga dan eerst even na wat er gebeurt met negatieve getallen.

elementen van $\mathbb{Z}$	$\ldots$	-4	-3	-2	-1	0	1	2	3	4 $\ldots$
modulo 3 (wiskundig)	$\ldots$	2	0	1	2	0	1	2	0	1 $\ldots$
%-operator in C++	$\ldots$	-1	0	-2	-1	0	1	2	0	1 $\ldots$

Om verwarring tussen berekeningen in $\mathbb{Z}$ en $\mathbb{Z}/_{n\mathbb{Z}}$ te voorkomen, gebruiken we waar nodig de $\equiv$-notatie in plaats van het gewone $=$-teken, eventueel aangevuld met de vermelding $\mod n$.

$+$ en $\times$ in $\mathbb{Z}$:	$3+5=8$	$3\times 5=15$
$+$ en $\times$ in $\mathbb{Z}_8$:	$3+5\equiv 0 \mod 8$	$3\times 5\equiv 7 \mod 8$

Om berekeningen in $\mathbb{Z}/_{n\mathbb{Z}}$ vlot te laten verlopen, wordt er (voor kleine n) gebruik gemaakt van optellings- en vermenigvuldigingstabellen. Voor $\mathbb{Z}/_{8\mathbb{Z}}$ worden deze tabellen:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Gezien het binaire geval $\boldsymbol{Z}/_{2\boldsymbol{Z}}$ zeer belangrijk is voor de informatica, hieronder de + en $\times$-tabellen voor $\boldsymbol{Z}/_{2\boldsymbol{Z}}$:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Twee bijkomende interpretaties van de optelling en vermenigvuldiging in $\boldsymbol{Z}/_{2\boldsymbol{Z}}$ springen hier in het oog:

- Staat 0 voor even en 1 voor oneven, dan lees je hier (o.a.) af dat oneven + oneven = even, en oneven $\times$ oneven = oneven.
- Anderzijds staan hierboven twee waarheidstabellen uit de logica (met 0=false, 1=true heb je respectievelijk de XOR-tabel en de AND-tabel).

In hoofdstuk 5 komen we uitgebreid terug op $\boldsymbol{Z}/_{n\boldsymbol{Z}}$, vanuit een meer theoretische invalshoek.

Oefening 1

Stel dat we de regels code van een programma oorspronkelijk in duizendtallen nummeren: 1000, 2000, 3000.... Op die manier laten we opeenvolgende inlassingen van bijkomende regels toe. Hoeveel lijnen code kan je tussen twee oorspronkelijke regels voegen, als
(a) we op voorhand weten waar al die regels code tussenmoeten.
(b) we bij inlassen van één lijn, niet weten waar de volgende zullen komen.

Oefening 2

Maak optellings- en vermenigvuldigingstabellen voor $\boldsymbol{Z}_{10}$ (of beter nog: laat een computerprogramma dit doen). Wat merk je op over de aanwezigheid van 0 en de andere getallen in de tabellen? Doe het zelfde voor $\boldsymbol{Z}_{11}$. Vergelijk.

Oefening 3

Los op: $6 \cdot x = 3 \bmod n$, met $n = 9, 10, 11, 12$. Wat merk je op over de oplossing van lineaire vergelijkingen in $\boldsymbol{Z}/_{n\boldsymbol{Z}}$?

Oefening 4

Bewijs dat $\sqrt{3}$ irrationaal is. Probeer op dezelfde manier te bewijzen dat $\sqrt{4}$ irrationaal is. Je bewijs zou ergens moeten stokken; waar?

Oefening 5

Geef voorbeelden van irrationale getallen x en y zodat
(a) $x + y$ en xy beide irrationaal zijn
(b) $x + y$ rationaal is, en xy irrationaal
(c) $x + y$ irrationaal is, en xy rationaal
(d) $x + y$ en xy beide rationaal zijn

Oefening 6

Toon aan dat

$$\begin{aligned}(a+b) \bmod n &\equiv a \bmod n + b \bmod n \\ (a \cdot b) \bmod n &\equiv (a \bmod n) \cdot (b \bmod n)\end{aligned}$$

Waarom mogen we niet schrijven $(a + b) \bmod n = a \bmod n + b \bmod n$? (Geef een tegenvoorbeeld.)

1.3 Radix r representatie van gehele getallen

We merkten al op dat de Romeinen een weinig efficiënte notatie gebruikten voor hun getallen.

1. Ten eerste kon de notatie van sommige getallen nogal lang uitvallen (bvb MCMLXXXVII).

2. Ten tweede kon je voor de bewerking (optelling, vermenigvuldiging) van twee grotere getallen niet terugvallen op eenvoudige algoritmes[2] om je resultaat te bekomen. Probeer maar een algoritme of computerprogramma te bedenken voor volgend rekensommetje: CCXLVI + DCCXVII = CMLXIII. En vergelijk dit met het eenvoudige
$$\begin{array}{r} 2\,4\,6 \\ +\;7\,1\,7 \\ \hline 9\,6\,3 \end{array}.$$
Die laatste notatie is niet alleen korter, het rekenwerk verloopt ook vlotter. Dit danken we aan de positionele notatie van ons Indisch-Arabisch getalsysteem: de positie waarop een cijfer staat, is beslissend voor de waarde die het cijfer voorstelt. Het cijfer 2 in 2345 is duizend keer meer waard dan het cijfer 2 in 5432, terwijl de laatste I in VIII voor evenveel meetelt als de eerste I in VIII.

3. Ten derde kon je één hoeveelheid op verschillende manieren uitdrukken, bvb. IV=IIII. In stelling 1.2 tonen we aan dat dit nooit kan bij positionele notatie.

De gebruikelijke positionele notatie is de radix-10-notatie: $1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$. Omdat niet elke positionele getalnotatie per se radix 10 heeft (denk maar aan de binaire code van de computer), staan we even stil bij de verschillende mogelijkheden. (De omzettingen

[2] te volgen procedure om gegeven input naar gewenste output om te vormen

tussen de verschillende stelsels, met name binair, octaal, decimaal, hexadecimaal, heb je al ingeoefend in het eerste jaar. We focussen hier vooral op de formele Σ-notatie, omdat die ons later nog van pas komt.)

Stel $n \in \mathbb{N}$. Willen we de getalwaarde van n voorstellen in een positioneel talstelsel in radix r, dan schrijven we n als

$$\begin{array}{lll} a_k a_{k-1} a_{k-2} \dots a_1 a_0 & \text{waarbij} & a_i \in \{0, 1, 2, \dots, r-1\} \\ & \text{en} & n = \sum_{i=0}^{k} a_i r^i \end{array}$$

Stelling 1.2. *De notatie $a_k a_{k-1} a_{k-2} \dots a_1 a_0$ van een getal n in een talstelsel met radix r is uniek.*

Bewijs Immers, stel dat deze niet uniek zou zijn, dan wordt n geschreven als $a_k a_{k-1} \dots a_1 a_0$ $= b_l b_{l-1} \dots b_1 b_0$. Onderstel dat $k = l$ (eventueel vullen we aan met leidende nullen). Berekenen we n mod r uit beide notaties, dan vinden we

$$\begin{array}{rcll} n \bmod r & = & (\sum_{i=0}^{k} a_i r^i) \bmod r & \\ & \overset{(1)}{\equiv} & \sum_{i=0}^{k} (a_i r^i \bmod r) & \text{(1): eigenschappen van } + \text{ en } \times \\ & \overset{(1)}{\equiv} & a_0 r^0 \bmod r & \text{in } \mathbb{Z}/_{n\mathbb{Z}}\text{; zie oef} \\ & \overset{(2)}{\equiv} & a_0 & \text{(2): } a_0 < r \end{array}$$

Maar ook

$$\begin{array}{rcll} n \bmod r & = & (\sum_{i=0}^{k} b_i r^i) \bmod r & \\ & \overset{(1)}{\equiv} & \sum_{i=0}^{k} (b_i r^i \bmod r) & \\ & \overset{(1)}{\equiv} & b_0 r^0 \bmod r & \\ & \overset{(3)}{\equiv} & b_0 & \text{(3): } b_0 < r \end{array}$$

Dus $a_0 \equiv n \bmod r \equiv b_0$, maar omdat $a_0 < r$ én $b_0 < r$, is $a_0 = b_0$.
Berekenen we $\left(\frac{n - a_0}{r}\right) \bmod r$ uit beide notaties:

$$\begin{array}{rcll} \left(\frac{n - a_0}{r}\right) \bmod r & = & (\sum_{i=1}^{k} a_i r^{i-1}) \bmod r & \\ & \overset{(1)}{\equiv} & \sum_{i=1}^{k} (a_i r^{i-1} \bmod r) & \\ & \overset{(1)}{\equiv} & a_1 r^0 \bmod r & \\ & \overset{(4)}{\equiv} & a_1 & \text{(4): } a_1 < r \\ \left(\frac{n - a_0}{r}\right) \bmod r & = & (\sum_{i=1}^{k} b_i r^{i-1}) \bmod r & \\ & & \dots & \\ & \equiv & b_1. & \end{array}$$

Dit kunnen we herhalen tot blijkt dat beide representaties $a_k a_{k-1} \dots a_1 a_0$ en $b_k b_{k-1} \dots b_1 b_0$ gelijk zijn. □

1.3.1 Omzetting tussen radixrepresentaties

Dit onderwerp kwam uitvoerig aan bod in het eerste jaar. Laten we toch nog even het belang van de regel van Horner zien. Willen we 54321_7 omzetten in decimaal stelsel, dan berekenen we

$$\begin{aligned} & 5 \cdot 7^4 + 4 \cdot 7^3 + 3 \cdot 7^2 + 2 \cdot 7 + 1 \quad (a)) \\ = \; & (((5 \cdot 7 + 4) \cdot 7 + 3) \cdot 7 + 2) \cdot 7 + 1 \quad (b)) \\ = \; & 13539_{10} \end{aligned}$$

Merk op dat de tweede berekeningswijze (b) minder grote tussenresultaten heeft, en minder vermenigvuldigingen gebruikt dan de eerste (a).

$$\begin{array}{rcl|rcl} 5 \cdot 7 \cdot 7 \cdot 7 \cdot 7 & = & 12005 & 5 \cdot 7 + 4 & = & 39 \\ 12005 + 4 \cdot 7 \cdot 7 \cdot 7 & = & 13377 & 39 \cdot 7 + 3 & = & 276 \\ 13377 + 3 \cdot 7 \cdot 7 & = & 13524 & 276 \cdot 7 + 2 & = & 1934 \\ 13524 + 2 \cdot 7 & = & 13538 & 1934 \cdot 7 + 1 & = & 13539 \\ 13538 + 1 & = & 13539 & & & \end{array}$$

1.4 Inductie

1.4.1 Bewijs via inductie

Uit de bespreking van de eigenschappen van $\mathbb{N}$, kwam het principe van de wiskundige inductie als belangrijkste naar voor. We kunnen dit als volgt formuleren:

> Laat S de *opvolgersfunctie* zijn, dus $S(n) = n + 1$.
> Dan kunnen we elk natuurlijk getal vanuit 0 bereiken, door S herhaaldelijk toe te passen.

Dit principe, geherformuleerd als bewijsmiddel:

> Elke eigenschap die voor 0 geldt, en die geldt voor de opvolger van een getal dat zélf die eigenschap bezit, geldt voor elk natuurlijk getal.

Het bewijs met inductie is een zeer sterk gereedschap. Dikwijls echter vallen bewijzen van deze soort vrij lang uit. Vooral dan is het belangrijk om de *structuur* van het bewijs *eerst* te noteren, en pas dan de concrete invulling te geven. Anders mondt 'bewijzen leren' gegarandeerd uit in 'van buiten blokken' - en dat is een trieste bezigheid, die ook niets oplevert (geen inzicht en geen punten).

Structuur van een bewijs met inductie

1. Eerst beslis je op welke VARIABELE je inductie toepast (op de parameter n in een formule; op de punten dan wel rechten van een meetkundige structuur; op het aantal elementen dan wel aantal deelverzamelingen van een verzameling;...) Laten we die variabele n noemen.
2. Dan leg je de BASIS: je bewijst de uitspraak voor kleine waarde(n) van n.
3. Dan start je met de STAP.
   (a) Daartoe formuleer je eerst de uitspraak voor n. Je mag onderstellen dat deze uitspraak WAAR is (zelfs al is dat niet bewezen!); het gaat hier om de INDUCTIEHYPOTHESE of inductie-onderstelling.
   (b) Daarna formuleer je de uitspraak voor $n + 1$. Dit is het TE BEWIJZEN.
   (c) Nu moet je bewijzen dat de uitspraak voor $n + 1$ volgt uit de uitspraak voor n. Uiteraard zal je daarvoor actief gebruik moeten maken van de uitspraak voor n!

Voorbeeld

Bewijs dat $2^{n+2} + 3^{2n+1}$ deelbaar is door 7.
VARIABELE In de formule staat slechts één variabele, dus we passen inductie

op n toe.
BASIS De eigenschap geldt voor $n = 0$ (ga na).
STAP
INDUCTIEHYPOTHESE
Er is gegeven dat $2^{n+2} + 3^{2n+1}$ deelbaar is door 7.
TE BEWIJZEN
We tonen aan dat $2^{(\mathbf{n+1})+2} + 3^{2(\mathbf{n+1})+1}$ ook deelbaar is door 7.

$$\begin{aligned} & 2^{(n+1)+2} + 3^{2(n+1)+1} \text{ is deelbaar door 7} \\ \Leftrightarrow\ & 2^{n+3} + 3^{2n+3} \text{ is deelbaar door 7} \end{aligned}$$

probeer het gegeven te gebruiken!!

$$\begin{aligned} \Leftrightarrow\ & 2 \cdot 2^{n+2} + 3^2 \cdot 3^{2n+1} \text{ is deelbaar door 7} \\ \Leftrightarrow\ & 2 \cdot \underline{(2^{n+2} + 3^{2n+1})} + \underline{7} \cdot 3^{2n+1} \text{ is deelbaar door 7} \end{aligned}$$

Gezien beide termen van de som deelbaar zijn door 7 (onderlijnde stukken), is de som deelbaar door 7. Quod erat demonstrandum, of $\square$.

Voorbeeld

Bewijs dat $n^3 < 3^n$, voor $n \geq 4$.
VARIABELE We passen inductie op n toe.
BASIS De eigenschap geldt voor $n = 4$ (ga na).
STAP Gegeven dat $n^3 < 3^n$, dan tonen we aan dat $(n+1)^3 < 3^{(n+1)}$.

De basiswaarde waarvan we bij inductie vertrekken hoeft dus niet per se 0 te zijn.
We kunnen het inductieprincipe ook uitbreiden naar dubbele, driedubbele,... inductie. Dan bewijzen we dat eigenschap P geldt voor $n + 2$, als ze geldt voor n én $n + 1$. We hebben dan wel 2 basiswaarden nodig, waarvoor P sowieso geldt.

Voorbeeld

De Fibonaccigetallen zijn gedefinieerd door $a_{n+2} = a_{n+1} + a_n$, met $a_1 = a_2 = 1$.
Bewijs dat de Fibonaccigetallen alle voldoen aan de ongelijkheid $a_{n+2} \geq (3/2)^n$.
VARIABELE Ook hier is er geen twijfel over de variabele: de enige die in aanmerking komt is n.
BASIS De eigenschap geldt voor de eerste Fibonaccigetallen ($a_1 = a_2 = 1$).
STAP Gegeven dat de eigenschap geldt voor n en $n + 1$, dan tonen we aan dat ze ook geldt voor $n + 2$. *Formuleer eerst beide gegevens; daarna het gevraagde; en probeer dan de afleiding van het gevraagde (=het bewijs).*

1.4.2 Recursieve definities

We zagen zonet dat een bewijs via inductie de eigenschap P voor het element $n+1$ kan bewijzen, steunend op eigenschap P voor element n. Niet alleen in bewijsvoeringen komen we deze inductieve of **recursieve** methode tegen, ook in **definities** van bepaalde (reeksen van) elementen. De Fibonaccigetallen zijn het bekendste voorbeeld: het is niet meteen duidelijk hoe het n-de element in de rij eruitziet; je kan het pas bepalen als alle elementen ervóór gekend zijn.[3] Je moet de rij dus bepalen via inductie (afleiding) uit vorige rij-elementen.

Voorbeeld

In de numerieke wiskunde worden dikwijls iteratieve methodes aangewend om, vertrekkende van een eerste ruwe afschatting, een steeds betere benadering te bekomen van de uiteindelijke oplossing van een vergelijking. Willen we bijvoorbeeld $\sqrt{10}$ berekenen, dan merken we op dat $\sqrt{10}$ de (positieve) oplossing is van de vergelijking $x^2 = 10$. Herschikken we dit:

$$\left.\begin{array}{rcl} x^2 &=& 10 \\ \Leftrightarrow \quad 2x^2 &=& x^2 + 10 \\ \Leftrightarrow \quad x &=& \frac{1}{2}(x + \frac{10}{x}) \end{array}\right| \begin{array}{l} +x^2 \\ \\ /2x \\ \\ \end{array}$$

Nemen we 4 als eerste ruwe afschatting, dan vinden we de recursieve definitie voor $\sqrt{10}$:

$$\begin{array}{rcl} a_0 &=& 4 \\ a_{n+1} &=& \frac{1}{2}(a_n + \frac{10}{a_n}) \end{array}$$

Merk op: dit komt overeen met de Newton-Raphson methode.

Oefening 7

Bewijs met inductie dat $n^3 - n$ deelbaar is door 6, voor elke gehele $n \geq 0$. Kan het ook zonder inductie? En wat voor negatieve n?

Oefening 8

Bewijs volgende gelijkheden met inductie. Stel een veralgemening van de formule voor, en bewijs deze ook met inductie.

$$\begin{array}{rcl} \sum_{i=1}^{n} i &=& \frac{1}{2}n(n+1) \\ \sum_{i=1}^{n} i(i+1) &=& \frac{1}{3}n(n+1)(n+2) \\ \sum_{i=1}^{n} i(i+1)(i+2) &=& \frac{1}{4}n(n+1)(n+2)(n+3) \end{array}$$

[3] Tenminste... zo lijkt het op het eerste zicht. Gebruik je een inductieve redenering, dan kan je wel een rechtstreekse formule vinden: $a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$.

1.4.3 Recursieve functies

Inductieve of beter: recursieve definities hangen zeer nauw samen met recursieve programma's. Een **recursief programma** of recursieve functie roept (delen van) zichzelf op: wil je met de functie-oproep `fibnr(5)` het vijfde Fibonaccigetal berekenen, dan zal deze functie het derde en vierde Fibonaccigetal berekenen en deze optellen. Hoewel... berekenen is teveel gezegd: er bestaat een methode om het derde en vierde Fibonaccigetal óp te roepen, nl. `fibnr(3)` en `fibnr(4)`. Meer gebeurt er niet binnen de functie `fibnr(n)`: `return fibnr(n-2)+fibnr(n-1)`. Vergeten we echter de inductiebasis niet: indien we als argument van de functieoproep `n=1` of `n=2` meegeven, krijgen we `fibnr(1)=1` en `fibnr(2)=1` in plaats van een (tot mislukking gedoemde) poging om `fibnr(n-2)` en `fibnr(n-1)` op te roepen en op te tellen.[4]
Let op: het enige dat een recursieve functie zal doen, is het probleem doorschuiven / delegeren naar het/de onderliggende niveau(s). Hoe die onderliggende niveaus hún probleem dan oplossen, is hun zaak - en vind je dus niet expliciet terug in de code.

We geven een programmeervoorbeeld aan de hand van de torens van Hanoï. "*De Torens van Hanoï* " is een klassieke denkpuzzel, bestaande uit 3 staven A, B, C en n schijven van verschillende diameter. Aan het begin van het spel staan de n schijven in piramidevorm (kleinste bovenaan) op staaf A. De puzzelaar wordt gevraagd om de toren te verplaatsen naar staaf B. Hierbij mag er slechts één schijf per keer verplaatst worden naar een andere staaf, en mag er nooit een grote schijf bovenop een kleine schijf gezet worden. De eenvoudigste oplossingen (voor $n = 2, 3$) kan je makkelijk uitschrijven. Voor $n = 4, 5, \ldots$ is het al wat moeilijker te volgen. Maar... als we de puzzel voor $n = 3$ kunnen oplossen, is de puzzel voor $n = 4$ eenvoudig op te splitsen in deelproblemen.
Verzet een stapel van 4 schijven van staaf A naar staaf B is immers gelijk aan:

1. verzet een stapel van ... schijven van staaf . naar staaf .
2. verzet ...
3. verzet ...

We zien dat het algoritme dat een stapel van n schijven verzet, beroep doet op het algoritme dat $n-1$ schijven verzet. Uiteraard zal dit door dezelfde functie of methode geïmplementeerd worden, maar met een andere parameterwaarde. Deze functie roept zichzelf dus op. Uit bovenstaande redenering volgt ook een recursieve formule voor het minimale aantal zetten a_n waarin de denkpuzzel met n schijven opgelost kan worden.

$$\begin{aligned} a_1 &= 1 \\ a_n &= 2a_{n-1} + 1 \end{aligned}$$

Oefening 9

> *Schrijf een recursieve functie* `hanoi(n,x,y)` *die n schijven van staaf x naar staaf y verzet. Vergeet vooral de inductiestap niet! Gebruik dit in een programma dat de puzzel voor willekeurige n oplost (zorg voor een bruikbare interface en leesbare output).*

[4] Programmeer dit eens, en laat *elke* oproep van de functie iets uitschrijven. Je zal merken dat dit de meest inefficiënte methode is om Fibonaccigetallen te berekenen. Maar wel recursief.

1.4.4 Lineaire inductie versus structurele inductie

Tot nu toe zagen we recursie als een lineair gegeven: een recursieve definitie of een recursief computerprogramma maakt gebruik van één (of meerdere) vorige uitkomsten — waarbij de opeenvolging van uitkomsten de telling of structuur van de gehele getallen volgden. Dit hoeft echter niet zo te zijn. In het hoofdstuk grafentheorie zien we niet-lineaire datastructuren zoals grafen of bomen. Kort geschetst: een **boom** is een verzameling elementen waarbij het (unieke) startelement een eindig aantal (gelijkwaardige) directe opvolgers heeft; en idem voor elk van die opvolgers. Bovendien geldt er dan nog een voorwaarde in verband met verboden 'lussen'. In de labosessies *Algoritmen I* die over bomen handelen, zal de voorkeur gegeven worden aan recursieve definities van klassen van bomen. De keuze voor deze recursieve definitie wordt dan consequent doorgetrokken in de structuur van lidfuncties/methodes voor deze klassen: deze zijn bij voorkeur recursief! De kunst is dan om elke recursieve methode zoveel mogelijk werk te laten doorschuiven aan zijn opvolgers, en enkel het hoogstnodige te behouden.

Hoofdstuk 2

Inleiding tot logica

Een wiskundig bewijs is een geheel van logische stappen die aantonen hoe een bewering A automatisch een bewering B impliceert. Hierbij veronderstelt men veelal dat er een zeer rigoureuze redeneerstijl gehanteerd werd. Toch is het — zelfs voor de meest gedetailleerde bewijsvoering — onmogelijk om werkelijk élke stap volledig met tekst en uitleg te verantwoorden. Kijk maar naar de bewijzen met inductie, of de bewijzen uit het ongerijmde uit hoofdstuk 1. In het begin probeerden we alle details toe te voegen, maar na een tijdje wordt dit te omslachtig en haalt het de aandacht van de hoofdzaken weg. Zo kan je het bewijs ook nooit onthouden[1]! Belicht je enkel de essentiële stappen in de redenering, dan zullen de details je later wel te binnen vallen.

Trekken we dit nu door naar de computer en het werk dat hij aflevert. Computerprogramma's bestaan ook uit een geheel van logische stappen om van een input A naar een output B te komen. Alleen... hier kan niets overgelaten worden aan parate kennis of intuïtie. Hier moet alles van a tot z exact vastgelegd worden. Voordeel is dat, eens het geheel van logische stappen tot in het kleinste detail correct opgesteld werd, de computer zeer snel en accuraat de stappen (herhaaldelijk) kan doorlopen. Elk van die stappen zal zeer eenvoudig zijn (een bit op 0 dan wel op 1 zetten), maar de manier waarop al die stappen gecombineerd worden is bepalend voor het succes.

Om ons te helpen de basisbewerkingen correct samen te stellen, hebben we logisch denkwerk nodig — logica. Er zijn twee formele systemen van logica te onderscheiden. Het eerste, *propositielogica*, houdt zich bezig met individuele proposities of uitspraken. Deze uitspraken worden als kleinste onderdeel van de logica beschouwd: ze zijn niet op te delen in kleinere stukken (of dat opdelen is toch niet wenselijk voor de beschouwde toepassing). Dit zal ook de logica zijn die best gebruikt wordt voor hardware design: ontwerpen van schakelingen en circuits. Het tweede systeem, de *predikatenlogica*, is een rijker systeem, omdat je hier kan werken met variabele startwaarden waarop je het logisch denkwerk loslaat. Dit systeem zal dan ook best aansluiten bij softwaredesign: ontwerpen van computerprogramma's. Gelukkig hebben beide systemen veel gemeen — en kunnen we ons permitteren om met het eenvoudigere werk te starten.

[1] Bewijzen die je van buiten leert kan je uiteraard *nooit* onthouden, dat is maar een lapmiddel. Slechts als je de logica in een bewijs hebt blootgelegd, maak je kans het werkelijk te onthouden. Dan ken je het bewijs van binnen.

2.1 Propositielogica

2.1.1 Formules van de propositielogica

Om te beginnen een omschrijving van wat we onder het begrip *formule* verstaan.

Definitie. *Een* **formule** *is een tekenreeks die aan een welbepaalde syntax voldoet, d.w.z. opgebouwd volgens een aantal welbepaalde regels.*

We bekommeren ons bij deze definitie dus niet om de mogelijke betekenis of inhoud van de tekenreeks; *formule* is een louter syntactisch begrip. Om welke regels het precies gaat, zal afhangen van de (programmeer-)taal waarin die formule opgesteld (en gebruikt) werd. Eens we de regels kennen, moeten we natuurlijk kunnen nagaan of ze ook allemaal gevolgd werden. Een computer doet dit werk aan de hand van een parser — die bij de gebruikte programmeertaal hoort. Er wordt een parse tree opgesteld, zodat de computer, na checken van de correcte syntax van de tekenreeks, ook meteen de structuur van de formule kan bepalen.

Propositielogica is een voorbeeld van een dergelijke taal. We omschrijven wat een formule van de propositielogica inhoudt. We vertrekken van een aantal individuele *propositionele variabelen*, nl. formules, die op zichzelf geen verdere analyse toelaten, en die we noteren met de letters $p, q, r, p_0, p_1, ...$ Merk op: misschien zijn de formules wel opgebouwd uit kleinere delen, maar propositielogica houdt zich niet met de verdere opsplitsing van p (of $q, ...$) bezig. Net zoals een scheikundige wel weet dat de moleculen waar hij mee werkt uit verschillende (sub)atomaire deeltjes bestaan — maar die verdere opsplitsing niet van nut vindt voor zijn werk.

Naast deze propositionele variabelen, kent de taal van de propositielogica nog deze symbolen:

$\neg$	niet
$\wedge$	en
$\vee$	of
$\bot$	contradictie
$\rightarrow$	als...dan
()	haakjes

Definitie. *Een willekeurige tekenreeks is een* **formule uit de propositielogica** *als ze voldoet aan volgende recursieve definitie:*

- *de tekenreeks is $\bot$ of is een propositionele variabele*
- *de tekenreeks is opgebouwd uit 1 of 2 formules φ en ψ, in één van volgende vormen:*

$$\neg\varphi \quad (\varphi \wedge \psi) \quad (\varphi \vee \psi) \quad (\varphi \rightarrow \psi)$$

Een tekenreeks is dus een formule als ze is opgebouwd volgens (een eindig aantal toepassingen van) de twee bovenstaande regels.

De Backus-Naur vorm[2] van deze recursieve definitie:

$$\begin{aligned} \text{formule} &:= \text{ondeelbare formule} \mid \neg \text{ formule} \mid (\text{formule} \wedge \text{formule}) \\ &\quad \mid (\text{formule} \to \text{formule}) \mid (\text{formule} \vee \text{formule}) \\ \text{ondeelbare formule} &:= \bot \mid p \mid q \mid r \mid p_0 \mid p_1 \mid ... \end{aligned}$$

Let op het gebruik van de haakjes bij de recursieve definitie van het begrip *formule* om onduidelijkheid te vermijden: $\varphi \to \psi \wedge \chi$ zou kunnen staan voor $((\varphi \to \psi) \wedge \chi)$ óf $(\varphi \to (\psi \wedge \chi))$. In de praktijk worden de haakjes wel eens weggelaten. Soms zijn ze niet nodig, bijvoorbeeld omdat $(\varphi \vee (\psi \vee \chi))$ en $((\varphi \vee \psi) \vee \chi)$ tóch equivalent zijn. In andere gevallen bieden bepaalde conventies omtrent interpretatie houvast; zo zal $\varphi \to \psi \wedge \chi$ staan voor $(\varphi \to (\psi \wedge \chi))$. Blijven er toch redelijk wat haakjes over, dan wordt er in praktijk gebruik gemaakt van verschillende soorten haakjes om de leesbaarheid te bevorderen ($(), [], \{\}, <>$). Officiëel echter (en voor verdere ontwikkeling van de theorie) worden er altijd haakjes gebruikt — ronde haakjes.

2.1.2 Haakjes en vorm van een formule

Gegeven een tekenreeks met enkel de symbolen die toegelaten zijn in de propositielogica. We stellen de parse tree [3] op van de formule, lettend op de haakjes.

$$(((((\neg p) \wedge q) \to r) \wedge (q \vee r)) \to ((p \vee r) \wedge (\neg q)))$$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
(	(	(	(	(	)	)	)	(	)	)	(	(	)	(	)	)	)

Elk koppel haakjes dat samenhoort, moet ook samen op een knoop van de boom gezet worden. We starten met een dummy-knoop — die later weg mag. Voor elk openend haakje maak je een nieuw kind aan voor de knoop waar je gebleven was. Stap voort naar die nieuwe knoop, en zet er links een '(' bij (of diens nummer). Voor elk sluitend haakje zet je een ')'-teken (of diens nummer) rechts naast de knoop waar je je bevond, en keer je terug naar de bovenliggende knoop. Het haakjespatroon is geldig als en slechts als we terug in de dummy-knoop geraken — die dan weggelaten wordt.

Om dan de eigenlijke parse tree te bekomen, voegen we nog bladeren toe aan de boom: die worden gelabeld met de propositionele variabelen. Daartoe zetten we eerst de symbolen $\neg, \wedge, \vee$ en $\to$ naast de knopen. Deze symbolen worden **operatoren** genoemd. Het eerste symbool, $\neg$, wordt toegepast op één formule en wordt **unair** genoemd. De andere symbolen $\wedge, \vee, \to$ worden toegepast op twee formules en zijn dus **binair**.

[2] De Backus-Naur vorm is een formalisme om de structuur van een taal vast te leggen. Alternatieven worden gescheiden door '|', definities worden aangegeven door ':='.

[3] Een tree of boom is een bepaalde structuur van elementen en verbindingen tussen een element en zijn (directe) opvolgers. De elementen of punten van de boom worden toppen of knopen genoemd. De unieke grootste knoop wordt de wortel genoemd. De knopen net onder een gegeven knoop worden zijn kinderen genoemd. De kinderloze knopen zijn per definitie de bladeren van de boom. Een exacte definitie vind je in het hoofdstuk over grafen.

Als je dit weet, vind je ook snel de plaats van de bladeren: knopen met symbolen $\wedge, \vee, \rightarrow$ hebben twee kinderen nodig, die met symbool $\neg$ slechts één.

We kunnen nu ook de deelformules afleiden uit de parse tree — hoewel dit de overzichtelijkheid niet ten goede komt.

Een laatste opmerking hierover, die je kan nagaan als je in de cursus *Algoritmen I* een boom leert doorlopen: in-order doorlopen komt overeen met de hiervoor geschetste notatie (met haakjes). Pre-order komt overeen met Poolse notatie, post-order komt overeen met omgekeerde Poolse notatie. Deze laatste is ook de werkwijze van een HP-rekentoestel met enter-toets. De formule uit de tekst wordt dan $p \ \neg \ q \wedge r \rightarrow q \quad r \vee \wedge \quad p \quad r \vee q \ \neg \ \wedge \rightarrow$ (zonder haakjes).

2.1.3 Betekenis van een formule en waarheidstabellen

Tot nu toe hielden we ons bezig met de *vorm* van een formule. De *inhoud* van een formule (nl. het feit of ze al dan niet waar is), kan je maar kennen als het waarheidsgehalte van alle propositionele variabelen $p, q, r, ...$ gekend is.

Definitie. *Een* **toekenning** v **van waar/vals-waarden aan de propositionele variabelen** $p_1, p_2, ..., p_n$ *(kortweg: een toekenning) is een functie die elke* p_i *een* waar- *dan wel een* vals-*waarde toekent. Zo kunnen we schrijven* $v(p_1, p_2, p_3) = (1, 0, 0)$, $v(p_1) = 1$, $v(p_2) = 0$,...

Hebben we een formule in de propositionele variabelen $p, q, r, ...$, dan zal elke toekenning aan $p, q, r, ...$ ook meteen een waarheidswaarde impliceren voor de formule. Sommen we alle mogelijke toekenningen (en hun gevolgen voor de formule) op, dan komen we aan een waarheidstabel.

Definitie. *Een* **waarheidstabel** *is een uitputtende opsomming van waarheidswaarden van de propositionele variabelen, met bijhorende waarheidswaarden van de formule(s) die uit die variabelen zijn samengesteld.*

In een waarheidstabel schrijven we een 1 indien de variabele of formule waar is, een 0 indien niet. (Andere conventies zijn uiteraard mogelijk: true/false, T/F, juist/fout,...) Doen we dit voor de basisformules met slechts één operator, dan krijgen we:

φ	$\neg\varphi$
1	0
0	1

φ	ψ	$\varphi \wedge \psi$	$\varphi \rightarrow \psi$	$\varphi \vee \psi$
1	1	1	1	1
1	0	0	0	1
0	1	0	1	1
0	0	0	1	0

De formule $\perp$ is altijd vals.

Stellen we een waarheidstabel op voor een formule, dan starten we in de linkerkolommen met de opsomming van mogelijke waarheidswaarden voor alle variabelen. Dit laat toe om achteraf snel te zien in welke toekenning de uiteindelijke formule waar dan wel vals is. (Om snel te kunnen vergelijken met je buren of met een gegeven oplossing, maak je ook best afspraken over de volgorde waarin de variabelen en toekenningen staan. Voorstel: variabelen alfabetisch; eerste mogelijke toekenning altijd 1 1 1 . . . 1 1 1.)

Is de formule vrij complex, noteer de formule dan met voldoende ruimte tussen de onderdelen. Noteer dan de waarheidswaarde van een deelformule onder de laatste operator die gebruikt werd bij vorming van de deelformule (zijn hoofdoperator). Geef eventueel met haakjes of in kleur aan, met welke kolommen je dient verder te werken. Zo vind je de waarheidswaarde van de volledige formule hieronder tussen vierkante haakjes; de laatste 2 tussenresultaten staan tussen ronde haakjes. Om het invullen (vooral van lange kolommen) te vergemakkelijken, kan je om de 2 of 4 rijen een hulplijn trekken.

p	q	r	$[\,p$	$\vee$	$(\,q$	$\wedge$	$r)\,]$	$\rightarrow$	$[\,(\neg\ r)$	$\rightarrow$	$(\,p$	$\vee$	$q)]$
1	1	1	1	1	1	1	1	1	0	1	1	1	1
1	1	0	1	1	1	0	0	1	1	0	1	1	1
1	0	1	1	1	0	0	1	1	0	1	1	1	0
1	0	0	1	1	0	0	0	1	1	0	1	1	0
0	1	1	0	1	1	1	1	1	0	1	1	0	1	1
0	1	0	0	0	1	0	0	1	1	0	1	0	1	1
0	0	1	0	0	0	0	1	1	0	1	1	0	0	0
0	0	0	0	0	0	0	0	1	1	0	0	0	0	0

Aan bovenstaand voorbeeld valt nog iets op te merken: blijkbaar is de vermelde formule altijd geldig, ongeacht het waarheidsgehalte toegekend aan p, q en r. We zeggen dan dat de formule geldig is, of een tautologie (van het Grieks: $\tau o\ \ \alpha \upsilon \tau o\ \ \lambda o \gamma o \varsigma$, hetzelfde woord).

φ is **geldig** φ is een tautologie	φ is onder alle toekenningen waar notatie: $\models \varphi$
φ is **tegenstrijdig** φ is een contradictie	φ is onder alle toekenningen vals $\neg\varphi$ is een tautologie
φ is **satisfiable**	φ is waar voor min 1 combinatie van waarheidsgehaltes van propositionele variabelen φ is niet contradictorisch

Definitie. *Twee formules φ en ψ zijn* **logisch equivalent** *als ze dezelfde waarheidstabel hebben, of nog: als de verzameling toekenningen waarvoor φ waar is, dezelfde is als die voor ψ. We schrijven $\varphi \equiv \psi$.*

Stel dat Γ een verzameling formules is. Dan is de formule φ een **logisch gevolg van** Γ *(of: $\Gamma \models \varphi$) als élke toekenning die alle leden van Γ geldig maakt, φ ook geldig maakt. Twee formules zijn dus logisch equivalent als en slechts als ze logisch gevolg zijn van elkaar.*

Voorbeeld

We lopen hier even vooruit op paragraaf 2.1.7, en geven een voorbeeldoefening. Voor $\Gamma = \{p \rightarrow q, q \rightarrow \neg r, r \rightarrow (p \vee s)\}$ en $\varphi = (\neg p \vee (q \wedge \neg r))$ bewijzen of weerleggen we dat $\Gamma \models \varphi$. (In paragraaf 2.1.7 zien we een handig hulpmiddel hiervoor, maar we proberen het eerst eens zonder.) Stel dat elke formule uit Γ waar is, maar φ niet. Dit zal tot een contradictie leiden, zodat we kunnen besluiten $\Gamma \models \varphi$. De waarheidswaarde van een formule ψ noteren we met $v(\psi)$. We onderstelden $v(\neg p \vee (q \wedge \neg r)) = 0$. Hieruit volgt $v(\neg p) = 0$ en $v(q \wedge \neg r) = 0$. Dus $v(p) = 1$. En $v(q) = 0$ of $v(r) = 1$. Uit $v(p \rightarrow q) = 1$ volgt $v(q) = 1$, dus $v(r) = 1$. Uit $v(q \rightarrow \neg r) = 1$ en $v(q) = 1$ volgt $v(r) = 0$: een contradictie.

Oefening 1

Schrijven we O voor '(' en S voor ')', stel dan de boom op die het volgende patroon van haakjes voorstelt:

1. *OOO S O S O SS OO S O S O SSS*
2. *OOOOO SS OO SSSS OOO SS OO SSSS*
3. *OO SS O SS OOO S O S O SS*
4. *OOOO S OO S O SS O SSS OO S O SSS*

Welk van de gegeven patronen kunnen het haakjespatroon van een formule uit de propositielogica zijn? Hoe zie je dat? (Geef een voorbeeld indien mogelijk.)

Oefening 2

Maak waarheidstabellen voor volgende formules. Welke zijn tautologieën, satisfiable en tegenstrijdig?

1. $\neg(p \vee q \vee \neg r) \wedge ((r \to p) \vee (r \to q))$
2. $(p \wedge \neg q) \to ((q \to r) \vee (p \to r))$
3. $(p \to (q \to (r \to s))) \to (((p \to q) \to r) \to s)$

Oefening 3

Zoek een propositionele formule met volgende parse tree (indien mogelijk).

Oefening 4

Toon aan dat volgende formules equivalent zijn (herken je de regels van De Morgan?).

1. $p \to q$ *en* $\neg q \to \neg p$
2. $\neg(p \vee q)$ *en* $(\neg p) \wedge (\neg q)$
3. $\neg(p \wedge q)$ *en* $(\neg p) \vee (\neg q)$

Oefening 5

Toon aan dat volgende formules tautologieën zijn.

1. *modus tollens* $[(p \wedge q) \wedge \neg q] \to \neg p$
2. *modus ponens* $[p \wedge (p \to q)] \to q$
3. *wet van syllogisme* $[(p \to q) \wedge (q \to r)] \to (p \to r)$
4. *wet van disjunctief syllogisme* $[(p \vee q) \wedge \neg p] \to q$

2.1.4 Afdoende verzamelingen operatoren

De keuze van de logische operatoren $\neg, \wedge, \vee$ en $\rightarrow$ hield rekening met twee zaken: de operatoren zijn makkelijk om te zetten naar (korte) operatoren uit de spreektaal: *niet*, *en*, *of*, *als...dan*, én we probeerden genoeg operatoren aan te bieden om de meest courante combinaties van uitdrukkingen vlot om te zetten. Toch kon het ook anders: strikt genomen konden we $\wedge$ en $\vee$ weglaten, gezien ze afkortingen zijn voor

$$\begin{array}{lcll} \varphi \wedge \psi & \equiv & \neg(\varphi \rightarrow (\neg\psi)) & \equiv \quad \neg(\psi \rightarrow (\neg\varphi)) \\ \varphi \vee \psi & \equiv & (\neg\varphi) \rightarrow \psi & \equiv \quad (\neg\psi) \rightarrow \varphi \end{array}$$

Deze equivalenties zijn vlot af te lezen van een waarheidstabel. We zeggen dat een verzameling propositionele operatoren **afdoend** is, als we voor elke mogelijke waarheidstabel gebaseerd op n logische variabelen $p_1, p_2, ..., p_n$ een formule kunnen vinden die enkel de gegeven operatoren gebruikt, en dezelfde waarheidstabel genereert.

Uit vorige redenering ($\wedge$ en $\vee$ kunnen uitgedrukt worden in functie van $\neg$ en $\rightarrow$), volgt dat $\{\neg, \rightarrow\}$ afdoend is indien $\{\neg, \rightarrow, \wedge, \vee\}$ dit is. We bewijzen in volgende paragraaf dat beide verzamelingen inderdaad afdoend zijn.

Andere vraag: waarom zouden we willen besparen op operatoren, als dit de uitdrukkingen ingewikkelder maakt? Omdat elke operator overeenkomt met een bepaalde poort in de schakelingenleer. En niet elke poort is altijd voorhanden.

2.1.5 Normaalvormen van een formule

Tot nu toe vertrokken we van een formule, en stelden we daarbij de waarheidstabel op. Het omgekeerde kan ook: stel dat je één of andere waarheidstabel krijgt, reconstrueer dan een formule die daarbij hoort.

Het is niet vanzelfsprekend dat dit zomaar lukt, zeker als we een waarheidstabel van lengte 2^n krijgen, met n groot. Probeer maar eens voor volgende waarheidstabellen: geef een (korte?) formule in de variabelen a en b, zodat de formule diezelfde waarheidstabel genereert.

a	b	tab 1	tab 2	tab 3	tab 4	tab 5	tab 6	tab 7	tab 8	tab 9	tab 10	tab 11	tab 12	tab 13	tab 14	tab 15	tab 16
1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Oplossing:

tabel 1	tabel 9
tabel 2	tabel 10
tabel 3	tabel 11
tabel 4	tabel 12
tabel 5	tabel 13
tabel 6	tabel 14
tabel 7	tabel 15
tabel 8	tabel 16

Je ziet dat je bij sommige tabellen toch even moet nadenken - en beslissen welke operatoren (of poorten) je nodig hebt. Meestal zijn er ook meerdere mogelijkheden, de ene al korter dan de andere. Kunnen we nu *altijd*, ook ingeval van n variabelen, een formule vinden? Het antwoord is gelukkig positief, al is de formule soms heel lang. (Inkorten kan, maar dat komt dan aan bod in paragraaf 2.1.6.)

Om de keuze voor de operatoren niet onnodig moeilijk te maken, kan het helpen om ons te beperken tot een niet te grote verzameling operatoren — die natuurlijk wel groot genoeg moet zijn om tot een oplossing voor het probleem te komen. We tonen aan dat $\{\neg, \wedge, \vee\}$, $\{\neg, \wedge, \vee, \rightarrow\}$ en $\{\neg, \rightarrow\}$ afdoend zijn. Ook enkele nieuwe operatoren doen hun intrede — operatoren die op zichzelf een afdoende verzameling vormen: { NAND } en { NOR }.

Om aan te tonen dat voor elke mogelijke waarheidstabel een formule bestaat die dezelfde uitkomsten heeft én enkel de operatoren $\neg, \wedge, \vee$ gebruikt, voeren we volgende terminologie in:

- een formule $\varphi_1 \vee \varphi_2 \vee ... \vee \varphi_n$ noemen we de **disjunctie** van $\varphi_1, \varphi_2, ..., \varphi_n$; φ_1 is de disjunctie van zichzelf. Merk op dat haakjes weggelaten mogen worden — gezien alle haakjespatronen hetzelfde logisch equivalent zullen geven.
- een formule $\varphi_1 \wedge \varphi_2 \wedge ... \wedge \varphi_n$ is de **conjunctie** van $\varphi_1, \varphi_2, ..., \varphi_n$.
- een formule in de vorm φ of $\neg\varphi$ is een **literal**.
- een formule staat in **disjunctieve normaalvorm** als ze een disjunctie is van conjuncties van literals.
- een formule staat in **conjunctieve normaalvorm** als ze een conjunctie is van disjuncties van literals.
- een **logische functie** is een *mogelijke waarheidstabel*. Hiermee bedoelen we dat voor een verzameling propositionele variabelen $\{p_1, p_2, ..., p_n\}$ elk van de 2^n mogelijke toekenningen aan $p_1, p_2, ..., p_n$ worden afgebeeld op de waarde 1 (waar) of 0 (vals).

  Voorbeeld van een logische functie op p, q, r:

p	q	r	
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0

zodat we kunnen afleiden dat $f(1,1,1) = 1$, $f(1,0,0) = 0$ enz.

Stelling 2.1. *Voor elke logische functie f is er een formule in disjunctieve normaalvorm wiens waarheidstabel gegeven is door f. Dus is er voor elke formule φ een formule χ in disjunctieve normaalvorm die logisch equivalent is met φ.*

Bewijs [4] We noteren de propositionele variabelen als p_j. Elke rij van de waarheidstabel van de logische functie f komt overeen met één toekenning v_i ($i : 1 \to 2^n$). Voor elk van deze rijen stellen we een conjunctie φ_{v_i} van literals op. Indien $v_i(p_j) = 1$, schrijven we p_j in de conjunctie. Indien $v_i(p_j) = 0$, schrijven we $\neg p_j$ in de conjunctie. Zo bekomen we de formule φ_{v_i}. (Voorbeeld: als $v_2(p_1, p_2, p_3, p_4) = (1, 0, 0, 1)$ wordt $\varphi_{v_2} = (p_1 \wedge \neg p_2 \wedge \neg p_3 \wedge p_4)$.) De clou van de zaak: de formule φ_{v_i} is *waar* in precies één rij van de waarheidstabel, nl. die gegeven door de toekenning v_i.

> Bewijs hiervan: De toekenning v_i maakt elke literal van φ_{v_i} *waar* (bij definitie), dus ook φ_{v_i} zelf. Elke toekenning v_k ($i \neq k$) zal minstens één propositionele variabele p_j een andere waarde toekennen: $v_k(p_j) \neq v_i(p_j)$. De literal in φ_{v_i} die correspondeert met p_j was zó gekozen dat φ_{v_i} *waar* werd onder v_i — dus vals onder v_k. Dus v_k maakt dat φ_{v_i} de waarde *vals* krijgt.

Nu stellen we de formule φ samen, door de juiste φ_{v_i} in disjunctie te zetten. Laat $w_1, w_2, ...w_m$ de toekenningen zijn waarvoor de logische functie f waarde 1 genereert. Bestaat er geen dergelijke functie, dan genereert f de waarde 0 voor elke lijn, dus stellen we $\varphi = \bot$. In het andere geval is $m \geq 1$. We stellen $\varphi = \varphi_{w_1} \vee \varphi_{w_2} \vee ... \vee \varphi_{w_m}$. Dan wordt de waarheidstabel van φ gegeven door de logische functie f.

> Bewijs hiervan: φ is waar zodra één van de φ_{w_k}'s waar is. Maar omdat φ_{w_k} enkel waar is in de rij die overeenstemt met de toekenning w_k, is φ enkel waar in de rijen waarin f de waarde 1 genereert.

[4] Nota voor wie thuis blokt: deze stelling levert een getrouwe weergave van het taalgebruik in wetenschappelijke artikels met wiskundige inslag. Zorg dat je dit niet vanbuiten, maar vanbinnen kent: eerst tot je laten doordringen wat de kern van de zaak is, en die dan in eigen bewoordingen formuleren. Een voorbeeld hiervan wordt in de les gegeven.

Gevolg 2.2. *De verzamelingen* $\{\neg, \wedge, \vee\}$, $\{\neg, \wedge, \vee, \rightarrow\}$ *en* $\{\neg, \rightarrow\}$ *zijn afdoende verzamelingen van operatoren.*

Bewijs De eerste verzameling is afdoend omdat elke disjuncte normaalvorm enkel deze operatoren nodig heeft, en omdat voor elke mogelijke waarheidstabel een formule in disjuncte normaalvorm bestaat (uit vorige stelling). Een verzameling operatoren die een afdoende verzameling omvat, is natuurlijk ook afdoend. En we hebben gezien dat $\wedge$ en $\vee$ uitgedrukt kunnen worden aan de hand van $\neg$ en $\rightarrow$ (nl. $\varphi \wedge \psi \equiv \neg(\varphi \rightarrow \neg\psi)$ en $\varphi \vee \psi \equiv \neg\varphi \rightarrow \psi$), zodat de derde verzameling ook afdoend is. □

Lemma 2.3. *Stel* φ, ψ *en* χ *logische formules of (door stelling hierboven) logische functies op een verzameling propositionele variabelen. Aan de hand van waarheidstabellen kunnen we volgende equivalenties nagaan:*

(a)	*commutativiteit*	$\varphi \wedge \psi \equiv \psi \wedge \varphi$
		$\varphi \vee \psi \equiv \psi \vee \varphi$
(b)	*associativiteit*	$(\varphi \wedge \psi) \wedge \chi \equiv \varphi \wedge (\psi \wedge \chi)$
		$(\varphi \vee \psi) \vee \chi \equiv \varphi \vee (\psi \vee \chi)$
(c)	*distributiviteit*	$\varphi \wedge (\psi \vee \chi) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$
		$\varphi \vee (\psi \wedge \chi) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \chi)$
(d)	*wetten van De Morgan*	$\neg(\varphi \wedge \psi) \equiv (\neg\varphi) \vee (\neg\psi)$
		$\neg(\varphi \vee \psi) \equiv (\neg\varphi) \wedge (\neg\psi)$
(e)	*dubbele negatie*	$\neg\neg\varphi \equiv \varphi$
(f)	*elementen 0 en 1*	$\varphi \vee \neg\varphi$ *is een tautologie*
		$\varphi \wedge \neg\varphi$ *is een contradictie*

Al deze eigenschappen samen drukken uit dat de verzameling van alle logische functies op een verzameling propositionele variabelen een Booleaanse algebra vormen. Een **Booleaanse algebra** is een structuur bestaande uit een verzameling $\mathbb{B}$ van elementen (waaronder een 0 en een 1), twee binaire operatoren $\wedge$ en $\vee$, en één unaire operator $-$. Voor elke $x, y, z \in \mathbb{B}$ moeten dan de vermelde eigenschappen gelden: commutativiteit, associativiteit, distributiviteit, regels van De Morgan, dubbele negatie (zie bovenstaand lemma). Sommige van deze eigenschappen zijn overbodig (want af te leiden uit de overige). We hadden ook een alternatieve definitie kunnen geven in termen van partiële ordening.

Stelling 2.4. *Voor elke logische functie* f *is er een formule in conjunctieve normaalvorm wiens waarheidstabel gegeven wordt door* f*. Dus bestaat er voor elke formule* φ *een formule in conjunctieve normaalvorm die logisch equivalent is met* φ*.*

Bewijs Stel g de logische functie die men bekomt door het omkeren van alle waarden die f geeft. Dan is er een formule ψ in disjuncte normaalvorm wiens waarheidstabel gegeven wordt door g. Bij definitie van g is de waarheidstabel van $\neg\psi$ gegeven door f. We zetten $\neg\psi$ om in conjunctieve normaalvorm:

$$\begin{array}{rrcl} & \psi & = & \psi_1 \vee \psi_2 \vee ... \vee \psi_m \quad \text{met } \psi_i = q_1 \wedge q_2 \wedge ... \wedge q_n \text{ voor literals } q_j \\ \Rightarrow & \neg\psi & = & \neg\psi_1 \wedge \neg\psi_2 \wedge ... \wedge \neg\psi_m \quad \text{met } \neg\psi_i = \neg(q_1 \wedge q_2 \wedge ... \wedge q_n) \\ & & & \qquad\qquad\qquad\qquad\qquad\qquad\quad = \neg q_1 \vee \neg q_2 \vee ... \vee \neg q_n \end{array}$$

Als q_j een literal is (dus propositionele variabele of de negatie ervan), dan is $\neg q_j$ het ook. We toonden hiermee aan dat $\neg\psi$ in conjunctieve normaalvorm staat. □

2.1.6 Logische poorten en Karnaugh-kaarten

In vorige paragraaf zagen we dat voor elke waarheidstabel een logische functie gevonden kan worden die enkel gebruik maakt van de operatoren $\{\neg, \wedge, \vee\}$. Om het in termen van digitale elektronica te zeggen: elke digitale component kan gerealiseerd worden aan de hand van invertoren, AND- en OR-poorten. Andere gekende poorten zijn XOR (exclusive or), XNOR ($\neg$ XOR), NAND ($\neg$ AND), NOR (noch A noch B). Is er ook een basispoort voor de $\rightarrow$-operator? (Merk op: deze is als enige niet-symmetrisch in de twee parameters.)

De twee poorten NAND en NOR zijn (de enige) universele poorten: je kan alle andere poorten maken door een combinatie van enkel NAND- of enkel NOR-poorten.

Stelling 2.5. *Voor elke logische functie f is er een formule die enkel gebruik maakt van de operator* NAND *en wiens waarheidstabel gegeven wordt door f.*

Bewijs Uit vorige stelling ($\{\neg, \wedge, \vee\}$ is een afdoende verzameling operatoren), en omdat $\neg, \wedge$ en $\vee$ herschreven kunnen worden in functie van NAND :

$$\begin{array}{rcll} \neg\varphi & \equiv & \varphi \text{ NAND } \varphi & \\ (\varphi \wedge \psi) & \equiv & \neg(\varphi \text{ NAND } \psi) & \equiv \ \ldots \\ (\varphi \vee \psi) & \equiv & (\neg\varphi) \text{ NAND } (\neg\psi) & \equiv \ \ldots \end{array}$$

□

Stelling 2.6. *Voor elke logische functie f is er een formule die enkel gebruik maakt van de operator* NOR *wiens waarheidstabel gegeven wordt door f.*

Bewijs Als oefening. □

Uit de digitale elektronica weet je dat een beperking op het aantal soorten poorten waarover je beschikt, de verbindingen van de poorten onderling veel ingewikkelder maakt. Ook de disjunctieve of conjunctieve normaalvorm, zoals die uit stellingen 2.1 en 2.4 volgt, is meestal veel langer dan nodig. Om een eenvoudige formule te vinden voor een gegeven logische tabel, kan de theorie van de Karnaugh-kaarten een welkom hulpmiddel zijn. Dit onderwerp werd reeds behandeld in de cursus digitale elektronica. Studenten die deze cursus in hun curriculum zagen, mogen meteen aan de oefeningen beginnen. Anderen hebben wellicht meer aan de theorie.

Gegeven een waarheidstabel op twee propositionele variabelen:

x	y	*output*
1	1	1
1	0	1
0	1	0
0	0	1

Passen we de methode uit stelling 2.1 toe om hier een logische uitdrukking voor te maken, dan krijgen we $(x \wedge y) \vee (x \wedge \neg y) \vee (\neg x \wedge \neg y)$. Dit is uiteraard veel te lang voor zo'n korte waarheidstabel. Herschikken we de tabel in een tweedimensionaal schema, dan krijgen we

	y	$\neg y$
x	1	1
$\neg x$	0	1

Elke cel komt overeen met een rij uit de waarheidstabel, dus met een conjunctie van twee literals. Disjunctieve samenstelling van de juiste conjuncties leverde ons de voorlopige (maar te lange) oplossing. Nemen we aangrenzende cellen echter samen (bvb de bovenste), dan komen we uit op volgende vereenvoudiging:

$$\begin{aligned}(x \wedge y) \vee (x \wedge \neg y) &= x \wedge (y \vee \neg y) \\ &= x \wedge 1 \\ &= x\end{aligned}$$

Op deze eenvoudige regel is de theorie van de Karnaugh-kaarten gebaseerd: baken gebieden af (rechthoekig of vierkant) door aangrenzende cellen samen te nemen. Cellen die aangrenzend zijn, zullen overeenkomen met conjuncties waarin slechts één van de literals verschilt (in ons voorbeeld: $x \wedge y$ te vergelijken met $x \wedge \neg y$). Nemen we de disjunctie van de conjuncties die bij cellen uit dit gebied behoren, dan zullen in de uitwerking ervan enkel de literals overblijven die in beide cellen gelijk waren. De andere literals verdwijnen: de waarheidswaarde van de bijhorende variabele deed er blijkbaar niet toe.

We kunnen dit uiteraard uitbreiden naar meerdere variabelen. Wel moeten we ervoor zorgen dat aangrenzende cellen in zo min mogelijk literals verschillen: dus niet het eerste schema, maar het tweede. (Merk op: beschouw het schema als een circulair iets; de linkercellen grenzen aan de rechtercellen, en de bovenste aan de onderste.)

	y z	y $\neg z$	$\neg y$ z	$\neg y$ $\neg z$
x u				
x $\neg u$		$x \wedge y \wedge$ $\neg z \wedge \neg u$	$x \wedge \neg y \wedge$ $z \wedge \neg u$	
$\neg x$ u				
$\neg x$ $\neg u$				

	y $\neg z$	y z	$\neg y$ z	$\neg y$ $\neg z$
x $\neg u$				
x u		$x \wedge y \wedge$ $z \wedge u$	$x \wedge \neg y \wedge$ $z \wedge u$	
$\neg x$ u				
$\neg x$ $\neg u$				

Hebben we een waarheidstabel in 4 variabelen overgebracht op de Karnaugh-kaart, dan kunnen we beginnen zoeken naar de beste manier om alle cellen waar een 1 in voorkomt, in rekening te brengen. Elk vierkant of rechthoekig gebied met zijde 1, 2 of 4 zal één conjunctie bijdragen in de uiteindelijke disjunctie die de logische functie uitmaakt. En hoe groter het gebied, hoe korter die conjunctie. Overlappingen zijn hierbij toegestaan - zelfs gewenst!

Voorbeeld

	r $\neg s$	r s	$\neg r$ s	$\neg r$ $\neg s$
p $\neg q$	0	0	0	1
p q	1	1	1	1
$\neg p$ q	0	1	1	0
$\neg p$ $\neg q$	0	0	0	0

Nemen we (van links naar rechts) een vierkant met zijde 1, daarnaast een vierkant met zijde 2, en tenslotte in de laatste kolom een rechthoek met zijde 2, dan krijgen we als uitdrukking $(p \wedge q \wedge r \wedge \neg s) \vee (q \wedge s) \vee (p \wedge \neg r \wedge \neg s)$. We kunnen echter beter doen: door het eerste vierkantje te vergroten tot de volledige tweede rij, verkorten we de eerste term in de disjunctie. Er komt dus $(p \wedge q) \vee (q \wedge s) \vee (p \wedge \neg r \wedge \neg s)$.

Oefening 6

De Shefferse streep is een operator genoteerd als '$|$' en gedefinieerd door de volgende waarheidstabel:

p	q	$p\|q$
1	1	0
1	0	1
0	1	1
0	0	1

Met welke reeds gekende operator komt deze operator overeen? Schrijf $\neg p$, $p \vee q$, $p \wedge q$ en $p \to q$ enkel met Shefferse strepen.

Oefening 7

Geef voor onderstaande Karnaugh-kaarten een zo kort mogelijke formule in disjunctieve normaalvorm.

	r $\neg s$	r s	$\neg r$ s	$\neg r$ $\neg s$
p	1	1	0	0
$\neg p$	1	1	1	0

	r $\neg s$	r s	$\neg r$ s	$\neg r$ $\neg s$
p $\neg q$	0	1	0	0
p q	1	1	0	1
$\neg p$ q	1	0	1	1
$\neg p$ $\neg q$	0	0	1	0

Oefening 8

Zoek een (niet te lange) uitdrukking die onderstaande waarheidstabel heeft.

p	q	r	s	*output*
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	1
1	0	1	1	0
1	0	1	0	1
1	0	0	1	0
1	0	0	0	1

p	q	r	s	*output*
0	1	1	1	0
0	1	1	0	1
0	1	0	1	1
0	1	0	0	1
0	0	1	1	1
0	0	1	0	1
0	0	0	1	0
0	0	0	0	1

Oefening 9

Maak van onderstaande uitdrukking een zo kort mogelijke disjunctieve normaalvorm *aan de hand van de gegeven Karnaugh-kaart (houd je aan de hoofdingen!).*

$$((\neg w) \to (x \wedge y)) \vee ((\neg w) \wedge (\neg x) \wedge z) \vee (\neg(y \to z))$$

	x y	x $\neg y$		
z w				
z $\neg w$				

2.1.7 Semantisch tableau

Tot nu toe zochten we naar formules die elkaars logisch equivalent zijn. Dit deden we door omzettingsregels toe te passen (zie o.a. lemma blz 28), of door enkel de waarheidstabel van de formule te beschouwen en aan de hand van Karnaugh-kaarten een korter alternatief te vinden. Het is echter ook van belang te kunnen uitmaken of een gegeven formule het logisch gevolg is van (een) andere formule(s). We herhalen: de formule φ is logisch gevolg van de verzameling formules Γ ($\Gamma \models \varphi$), als élke toekenning die alle elementen van Γ geldig maakt, ook φ geldig maakt. Om na te gaan of φ logisch gevolg is van Γ, kunnen we

1. alle mogelijke toekenningen v voor de propositionele variabelen $p_1, p_2, ...$ opsommen en hun gevolgen controleren voor Γ en φ.
2. gericht zoeken naar een toekenning die de uitspraak $\Gamma \models \varphi$ weerlegt.

De eerste methode werkt, maar is allesbehalve elegant. De tweede methode is veel boeiender — en we kunnen hier gebruik maken van een semantisch tableau om ervoor te zorgen dat onze zoektocht effectief gericht verloopt.

Een **semantisch tableau** is een boomstructuur die, vertrekkende van de gekende waarheidswaarde van een (ingewikkelde) formule, alle corresponderende toekenningen v voor de propositionele variabelen $p_1, p_2, ...$ op een systematische manier in kaart brengt. Daarbij komt elke formule (samengesteld, literal of logische variabele) die *waar* is links van een vertikale streep te staan; elke formule die *onwaar* is staat rechts. De vertikale lijn kan opgesplitst worden in twee verschillende vertikale lijnen (boomstructuur), om een gegeven situatie op te splitsen in twee deelsituaties (het gaat hier dus om een gevallenstudie). Elke deelsituatie (of tak) wordt verder opgesplitst, tot er een contradictie voorkomt op de tak (een variabele die zowel waar als onwaar is), óf tot alle samengestelde formules vervangen werden door hun samenstellende variabelen. In het eerste geval zegt men dat **de tak sluit**, in het andere geval is **de tak open**.

Op volgende bladzijde kan je het semantisch tableau voor de basisoperatoren $\{\neg, \wedge, \vee, \rightarrow\}$ aanvullen.

Met een semantisch tableau kan je dus elke vraag van de volgende vorm oplossen: gegeven een formule waarvan ik weet/onderstel dat ze een bepaald waarheidsgehalte (0 of 1) heeft, welke toekenningen komen daar dan mee overeen?

Hier zullen we een semantisch tableau gebruiken om aan te tonen dat $\Gamma \models \varphi$ waar is, of nog: $(\gamma_1 \wedge \gamma_2 \wedge ...\gamma_n) \rightarrow \varphi$ is waar. Hiertoe gebruiken we een bewijs uit het ongerijmde. Stel dat onze uitspraak niet zo is, dus $\Gamma \models \varphi$ is vals, welke toekenningen vinden we dan aan de hand van het tableau dat start met $\Gamma \models \varphi$ aan de rechterkant van de streep?

- Vinden we op elke tak van het bijhorende semantisch tableau een contradictie, dan kunnen we besluiten dat $\Gamma \models \varphi$. Immers, er bestaat dan geen enkele toekenning v van waarheidswaarden voor de logische variabelen $p_1, p_2, ...$, waarvoor $\Gamma \models \varphi$ onwaar is.

- Houden we nog minstens één open tak over, dan hebben we meteen een tegenvoorbeeld van de uitspraak $\Gamma \models \varphi$: een toekenning v waarvoor $\Gamma \models \varphi$ onwaar is. Dus $\Gamma \not\models \varphi$.

is	WAAR	ONWAAR
¬A		
A∧B		
A∨B		
A→B		

Oefening 10

Toon met een semantisch tableau aan — of weerleg:

1. $\{p \to q, q \to r, r \to s\} \models p \to s$
2. $\{p \vee q, p \wedge q\} \models q \to r$
3. $\{p \to q, \neg p\} \models \neg q$
4. $\{p_0 \to p_1, p_1 \to p_2, p_2 \to p_3, ...\} \models p_0 \vee p_5$

Oefening 11

Zet volgende bewering om in de taal van de propositielogica. Definieer daartoe eerst de nodige propositionele variabelen. Ga dan na of de bewering waar of vals is (gebruik een semantisch tableau).

> *Speelde de kat viool of sprong*
> *de koe over de maan, dan lachte*
> *de hond. Lachte de hond, dan*
> *liep de lepel weg met de vork.*
> *Maar de lepel liep niet weg*
> *met de vork. Dus speelde de kat*
> *geen viool.*

2.2 Predikatenlogica

In dit onderdeel stappen we van de propositielogica over op de predikatenlogica. Een propositie is een uitspraak of stelling (bvb *'de kat speelt viool'*), waaraan je een waarheidswaarde kan toekennen. We scheiden nu het onderwerp (*'de kat'*) van het predikaat in de gegeven propositie. Een predikaat is een eigenschap, of 'datgene wat van iets gezegd wordt'. Noch het onderwerp, noch het predikaat kan op zich een waarheidswaarde aannemen. Het geheel, de propositie, echter wel.

De predikatenlogica wil het mogelijk maken de geldigheid van uitspraken te linken aan de *variabelen* (of onderwerpen) waarover ze spreken. Zo kan je van de uitspraak '$x < 5$' niet zeggen of ze waar is, tenzij je de expliciete waarde van x kent. Diezelfde uitspraak met een kwantor ervoor, bijvoorbeeld $(\exists x)(x < 5)$, kan je wél een waarheidswaarde toekennen (zónder daarom aan x een expliciete waarde toegekend te hebben).

De extra symbolen die we nodig hebben om de propositielogica uit te bouwen tot predikatenlogica:

universele kwantor	$\forall$
existentiële kwantor	$\exists$
constanten	$\underline{a}, \underline{b}, \underline{c}, \ldots$
variabelen	$x, y, z, \ldots$
functiesymbolen	$\underline{f}(), \underline{g}(), \ldots$
relatiesymbolen	$\underline{P}(), \underline{Q}(), \underline{R}(), \ldots$

De variabelen $x, y, z \ldots$ kunnen waarden aannemen in een bepaalde verzameling (het domein), zo bijvoorbeeld $x \in \mathbb{N}$, $x < 5$ of $\underline{D}(x)$ waarbij $\underline{D}()$ staat voor *is een diersoort*.

De constanten staan voor bepaalde vaste elementen van het domein, zo bijvoorbeeld 5 of $\underline{a}$ waarbij $\underline{a}$ staat voor *aap*.

Functiesymbolen staan voor bepaalde functies of operaties, zo bijvoorbeeld $\underline{\sin}()$ en $\underline{\times}$.

Relatiesymbolen staan voor bepaalde relaties die tussen elementen van het domein gelden, zo bijvoorbeeld $\underline{\mathrm{St}}(.,.)$ voor *stamt af van* of $\underline{V}(.)$ voor *is viervoud*.

Houden we alles heel formeel, dan gebruiken we voor variabelen, constanten, functies en relatiesymbolen enkel enkelvoudige letters. Willen we de leesbaarheid bevorderen, dan gebruiken we afkortingen of symbolen ($\underline{\sin}$, $\underline{\times}$, $\underline{\mathrm{St}}$).

Het aantal parameters dat een functiesymbool of relatiesymbool verlangt, wordt best ook gespecifieerd (of leid je uit de betekenis af).

Het verschil tussen een relatie en een functie:

- Een **relatie** tussen $2, 3, 4, \ldots$ elementen van een domein (of zelfs op 0 of 1 element van een domein), is een eigenschap die al dan niet geldig is. Een relatiesymbool mét zijn parameters kan je dus vervangen door *waar* dan wel *vals*.

- Een **functie** is een regel die elementen van het domein afbeeldt op elementen van het domein. Een functiesymbool mét zijn parameters kan je dus vervangen door een element van het domein waarvan sprake.

In de propositielogica bestonden de formules uit operatoren en logische variabelen, opgebouwd volgens een recursieve structuur. In de predikatenlogica worden formules ook recursief gedefinieerd. Maar eerst hebben we de (recursieve) definitie van het begrip *term* nodig.

Definitie. *Een willekeurige tekenreeks is een* **term uit de predikatenlogica** *als ze voldoet aan deze recursieve definitie:*

- *de tekenreeks is een variabele of constante*
- *de tekenreeks is van de vorm* $\underline{f}(t_1, \ldots, t_m)$ *met* $\underline{f}$ *een functiesymbool met* m *parameters, en* $t_1, \ldots, t_m$ *termen.*

Met andere woorden: termen zijn mogelijke elementen uit het domein.

Definitie. *Een willekeurige tekenreeks is een* **formule uit de predikatenlogica** *als ze voldoet aan deze recursieve definitie:*

- *de tekenreeks is* $\bot$
- *de tekenreeks is van de vorm* $\underline{R}(t_1, \ldots, t_m)$ *met* $\underline{R}$ *een relatiesymbool met* m *parameters en* $t_1, \ldots, t_m$ *termen*
- *de tekenreeks is van één van volgende vormen*

  $$(\neg A) \quad (A \wedge B) \quad (A \to B) \quad (A \vee B) \qquad (\exists x)(A) \qquad (\forall x)(A)$$

  met A *en* B *formules en* x *een variabele.*

Met andere woorden: formules zijn uitspraken die de waarden *waar/vals* kunnen aannemen. De eerste twee soorten formules worden **atomaire formules** van de predikatenlogica genoemd.

Oefening 12

Gegeven een codefragment C++/java. Onderlijn alle termen in blauw, alle formules in groen (wees nauwkeurig).

```
if (c < d) {
    x = y;
    if (a%7 == 0)
         d=d+1;
}
```

2.2.1 Zinsontleding in predikatenlogica

Willen we predikatenlogica gebruiken om bepaalde uitspraken met wiskundige zekerheid te verifiëren, dan moeten we eerst de uitspraken leren omzetten in de vorm van een formule uit de predikatenlogica. Enkele voorbeelden.

Voorbeeld

Iedereen sprak Frans of Engels.
Op het eerste zicht aanwezig: $\forall$ (*iedereen*) en $\vee$ (*of*).
Unaire predikaten: $\underline{F}(x)$ (x *spreekt Frans*)
$\underline{E}(x)$ (x *spreekt Engels*)
Wat nog ontbreekt, maar af te leiden valt uit de contekst (nl. dat niet iedereen op de gehele wereld Frans of Engels spreekt): het gaat hier om de personen aanwezig op een bepaalde plaats of tijdstip. Drukken we dit uit met $\underline{A}(x)$ voor x *was aanwezig*), dan krijgen we

$$(\forall x)(\underline{A}(x) \to \underline{F}(x) \vee \underline{E}(x))$$

Voorbeeld

Er was iemand die Roemeens of Russisch sprak.

$$(\exists x)(\underline{A}(x) \wedge (\underline{Ro}(x) \vee \underline{Ru}(x)))$$

Merk op: na de universele kwantor gebruiken we $\to$, na de existentiële kwantor gebruiken we $\wedge$. Dit is geen wet van Meden en Perzen, eerder conventie.

Voorbeeld

Elke persoon die geen Frans sprak, had een persoonlijke tolk bij die Frans en Engels sprak.

$$(\forall x)(\neg\underline{F}(x) \to (\exists y)(\underline{F}(y) \wedge \underline{E}(y) \wedge \underline{T}(y, x)))$$

met $\underline{T}(a, b)$ voor a *is persoonlijke tolk van* b.

Voorbeeld

You can fool some people all of the time,
you can fool all people some of the time,
but you can't fool mum.

We stellen

$\underline{m}$	*mum*
$\underline{P}(x)$	x *is een persoon*
$\underline{T}(t)$	t *is een tijd*
$\underline{L}(x, t)$	*je kan liegen tegen* x *op tijdstip* t

Dan krijgen we

$$\begin{array}{ll} & (\exists x)(\underline{P}(x) \wedge (\forall t)(\underline{T}(t) \rightarrow \underline{L}(x,t))) \\ \wedge & (\forall x)(\underline{P}(x) \rightarrow (\exists t)(\underline{T}(t) \wedge \underline{L}(x,t))) \\ \wedge & (\forall t)(\underline{T}(t) \rightarrow \neg \underline{L}(\underline{m},t)) \end{array}$$

Hier zie je dat de twee laatste regels in tegenspraak zijn met elkaar, gezien $\underline{P}(\underline{m})$! In de regel *you can fool all people some of the time*, moet je bij omzetting naar de formele taal van de logica reeds aangeven dat *all people* eigenlijk *all people except mum* moet zijn. Maar dan is de pointe van de uitspraak natuurlijk verdwenen... De tweede regel wordt dus (zet $x \neq m$ nog om naar meer formele notatie):

$$\wedge(\forall x)((\underline{P}(x) \wedge x \neq \underline{m}) \rightarrow (\exists t)(\underline{T}(t) \wedge \underline{L}(x,t)))$$

2.2.2 Gebonden en vrije variabelen

Het gebruik van de kwantoren $\forall$ en $\exists$ is essentieel voor de predikatenlogica. Je kan van een uitspraak '$x < 5$' niet zeggen of ze waar is, gezien x nog vrij is om alle waarden van het domein aan te nemen. In de gekwantificeerde formules $(\exists x)(x < 5)$ en $(\forall x)(x < 5)$ is x al *aan voorwaarden in verband met het domein onderworpen*: x is nu een gebonden variabele. De twee laatste formules hebben een welgedefinieerde waarheidswaarde. Het is belangrijk een verschil te maken tussen vrije en gebonden variabelen; te vergelijken met de globale en lokale variabelen in een computerprogramma.[5]

De **scope** van een kwantor $\forall x$ of $\exists x$ wordt als volgt gedefinieerd: vormen we vanuit de formule (φ) de formule $(\forall x)(\varphi)$ of $(\exists x)(\varphi)$, dan is φ de scope van $\forall x$ respectievelijk $\exists x$.

Een variabele x is dan gebonden als x onmiddellijk na $\forall/\exists$ komt, of in de scope van een kwantor $\forall x/\exists x$. Anders is de variabele vrij.

Er is geen enkele formele regel die ons verbiedt een variabele zowel in vrije als gebonden vorm te gebruiken binnen dezelfde formule (bijvoorbeeld $[(\exists x)\underline{P}(x,y)] \wedge \underline{Q}(x,z)$). In regel vermijden we dit om evidente redenen. Het is dan beter om de vrije variabele x te vervangen door een variabele met een andere naam, bijvoorbeeld t. We substitueren t dan in de (vrije) variabele x.

[5] Voor wie thuis blokt: informeer je goed over wat in de les behandeld werd.

Lemma 2.7. *Gegeven formules φ en ψ,*
een variabele x die niet gebonden voorkomt in φ, en helemaal niet voorkomt in ψ,
en een variabele y die voorkomt in φ noch ψ.
Dan geldt er

$$\begin{array}{ll}
(a) & \neg\forall x\varphi(x) \equiv \exists x\neg\varphi(x) \\
 & \neg\exists x\varphi(x) \equiv \forall x\neg\varphi(x) \\
(b) & (\forall x\varphi) \wedge \psi \equiv \forall x(\varphi \wedge \psi) \\
 & (\exists x\varphi) \wedge \psi \equiv \exists x(\varphi \wedge \psi) \\
(c) & (\forall x\varphi) \vee \psi \equiv \forall x(\varphi \vee \psi) \\
 & (\exists x\varphi) \vee \psi \equiv \exists x(\varphi \vee \psi) \\
(d) & (\forall x\varphi) \to \psi \equiv \exists x(\varphi \to \psi) \\
 & (\exists x\varphi) \to \psi \equiv \forall x(\varphi \to \psi) \\
(e) & \psi \to (\forall x\varphi) \equiv \forall x(\psi \to \varphi) \\
 & \psi \to (\exists x\varphi) \equiv \exists x(\psi \to \varphi) \\
(f) & \forall x\varphi(x) \equiv \forall y\varphi(y) \\
 & \exists x\varphi(x) \equiv \exists y\varphi(y)
\end{array}$$

Bewijs Oefening. □

Een formule van de predikatenlogica staat in **prenexnormaalvorm** als ze van de vorm

$$(Q_1x_1)(Q_2x_2)\dots(Q_nx_n)\psi$$

is, met ψ kwantorvrij, en elke Q_r gelijk aan $\forall$ of $\exists$.

Stelling 2.8. *Elke formule φ van de predikatenlogica is logisch equivalent met een formule in prenexnormaalvorm.*

Bewijs met inductie op de lengte van φ.
BASIS Stel φ is een kwantorvrije formule. In dat geval is de stelling triviaal.
STAP We onderstellen dat de stelling geldig is voor elke formule die korter is dan φ (d.w.z. elke formule korter dan φ kan geschreven worden in prenexnormaalvorm). Daaruit leiden we af dat φ geschreven kan worden in prenexnormaalvorm.
Als φ niet kwantorvrij is, dan kan φ geschreven worden als (zie recursieve definitie van het begrip *formule* uit de predikatenlogica):

$$\neg\varphi_1 \quad (\varphi_1 \wedge \varphi_2) \quad (\varphi_1 \vee \varphi_2) \quad (\varphi_1 \to \varphi_2) \quad (\exists x)\varphi_1 \quad (\forall x)\varphi_1$$

met φ_1 en φ_2 korter dan φ — dus bij inductiehypothese zelf equivalent met een formule in prenexnormaalvorm.

- Stel $\varphi \equiv \neg\varphi_1$ en $\varphi_1 \equiv (Q_1x_1)(Q_2x_2)\dots(Q_nx_n)\psi$ met ψ kwantorvrij. Veranderen we de

kwantor Q_i (van $\forall$ naar $\exists$ en omgekeerd), dan noteren we het resultaat met $\overline{Q_i}$.

$$\begin{array}{rcl} \Rightarrow & \varphi & \equiv \neg((Q_1x_1)(Q_2x_2)\dots(Q_nx_n)\psi) \\ \overset{(a)}{\Rightarrow} & \varphi & \equiv (\overline{Q_1}x_1)\neg((Q_2x_2)\dots(Q_nx_n)\psi) \\ \overset{(a)}{\Rightarrow} & \varphi & \equiv (\overline{Q_1}x_1)(\overline{Q_2}x_2)\neg(\dots(Q_nx_n)\psi) \\ & \vdots & \\ \overset{(a)}{\Rightarrow} & \varphi & \equiv (\overline{Q_1}x_1)(\overline{Q_2}x_2)\dots\neg((Q_nx_n)\psi) \\ \overset{(a)}{\Rightarrow} & \varphi & \equiv (\overline{Q_1}x_1)(\overline{Q_2}x_2)\dots(\overline{Q_n}x_n)\psi) \end{array}$$

waarbij we lemma 2.7 deel *(a)* gebruikten. Dus is φ te schrijven in prenexnormaalvorm.

- Stel $\varphi \equiv \varphi_1 \wedge \varphi_2$, $\varphi_1 \equiv (Q_1x_1)(Q_2x_2)\dots(Q_nx_n)\psi_1$ en $\varphi_2 \equiv (Q'_1y_1)(Q'_2y_2)\dots(Q'_my_m)\psi_2$. Omdat alle x_i gebonden zijn in φ_1, en alle y_i gebonden zijn in φ_2, kunnen we ze door nieuwe variabelen vervangen indien nodig — zodat ze allemaal verschillend zijn. De formules ψ_1 en ψ_2 zijn kwantorvrij, dus ψ_2 zal $x_1, \dots, x_n$ niet bevatten, en ψ_1 zal $y_1, \dots, y_m$ niet bevatten.

$$\overset{(b)}{\Rightarrow} \quad \varphi_1 \wedge \varphi_2 \quad \equiv \quad (Q_1x_1)\dots(Q_nx_n)(Q'_1y_1)\dots(Q'_my_m)(\psi_1 \wedge \psi_2)$$

- Stel $\varphi \equiv \varphi_1 \vee \varphi_2$: analoog.
- Stel $\varphi \equiv \varphi_1 \to \varphi_2$: analoog.
- Stel $\varphi \equiv (Qx)\varphi_1$ (met Q gelijk aan $\exists$ of $\forall$) en $\varphi_1 \equiv (Q_1x_1)\dots(Q_nx_n)\psi_1$. Dan is $\varphi \equiv (Qx)(Q_1x_1)\dots(Q_nx_n)\psi_1$ geschreven in prenexnormaalvorm.

□

Oefening 13

Zoek een prenexnormaalvorm voor

- $[(\neg(\forall x)P(x,y)) \wedge Q(x)] \wedge \neg(((\forall z)R(z)) \wedge S(w))$
- $(\forall x)(P(x,y) \to Q(z)) \vee \exists x(R(z) \to \forall y S(x,y,z))$

2.3 Logica en wiskundige bewijsvoering

Logica formeel beschrijven is één zaak, mét logica zaken formeel beschrijven een andere. Als afsluiter gaan we na waar de logica ons een handje toesteekt als het gaat om (al dan niet wiskundige) bewijzen op te stellen. We onderscheiden 2 types stellingen: $p \to q$ en $p \leftrightarrow q$. We geven een lijstje van mogelijke bewijsmethodes voor de stellingen van het type $p \to q$ (de bewijsmethodes voor stellingen van het type $p \leftrightarrow q$ zijn hierop terug te voeren). Elk bewijs en elk deelbewijs in deze cursus is onder te brengen bij één van deze methodes. Daarom is het belangrijk deze methodes goed te kunnen onderscheiden. Weet je immers wat het gegeven is (p), wat je moet bewijzen (q) én welke bewijsmethode je toepast (bvb. $\neg q \to \neg p$), dan heb je al de helft van het werk verricht.

2.3.1 Soorten bewijsmethodes voor de stelling $p \to q$

Definitie. *Het bewijs van een stelling $p \to q$ is een opeenvolging van logische argumenten om aan te tonen dat de formule $p \to q$ (óf elke formule die hier logisch equivalent mee is), een tautologie is.*

Er zijn veel proposities die logisch equivalent zijn met de uitspraak $p \to q$. We sommen er een vijftal op: deze komen telkens overeen met een bewijsmethode. Als je kan aantonen dat de gekozen logisch equivalente propositie waarheidswaarde 1 heeft, dan heeft ook $p \to q$ de waarheidswaarde 1. En dan is het bewijs van de stelling $p \to q$ geleverd.

(1) $p \to q$
De meest natuurlijke vorm van een (wiskundig) bewijs is het **directe bewijs**. We nemen aan dat $v(p) = 1$, en tonen dat $v(q) = 1$. Hierbij wordt dikwijls de wet van het syllogisme gebruikt (zie oefening 2.1.3).

(2) $\neg q \to \neg p$
Een tweede type bewijsvoering baseert zich op de wet van de **contrapositie**: $p \to q$ en $\neg q \to \neg p$ zijn logisch equivalent. Een direct bewijs van $\neg q \to \neg p$ is dus geldig als bewijs van de uitspraak $p \to q$.

(3) $((p \wedge \neg q) \to r) \wedge \neg r$
Het derde type, het **bewijs uit het ongerijmde**, steunt op volgende logische equivalenties:

$$\begin{aligned} [(p \wedge \neg q) \to r] \wedge [\neg r] &\equiv \neg(p \wedge \neg q) \\ &\equiv \neg p \vee q \\ &\equiv p \to q \end{aligned}$$

In woorden: we tonen de stelling $p \to q$ aan door aan te nemen dat p en $\neg q$ waar zijn, en een ongeldige uitspraak r (een contradictie) af te leiden. Omdat $(p \wedge \neg q) \to r$ waar is, en r vals, kunnen we besluiten dat $(p \wedge \neg q)$ vals is. Maar dan is $\neg(p \wedge \neg q)$ waar, en dat is logisch equivalent met wat we moesten aantonen: $p \to q$ is waar.

(4) Bewijs door **inductie** bespraken we reeds in hoofdstuk 1. Vergeet hier niet te vermelden waaróp je inductie toepast!

(5) Voor veel bewijzen (cursus *Algoritmen*!) splitsen we het te bewijzen op in delen: we voeren een **gevallenstudie** door. (Voorbeeld: aparte bewijsvoering voor de even en oneven gevallen.) Indien $q \equiv q_1 \wedge q_2$, zal $(p \to q_1) \wedge (p \to q_2) \equiv p \to (q_1 \wedge q_2)$ logisch equivalent zijn met $p \to q$.

En tot slot: uiteraard stoot een wiskundige die dénkt dat hij een stelling gevonden heeft, wel eens op verrassingen als hij zijn vermoeden (conjecture) tracht te bewijzen. Zulke verrassing kan een **tegenvoorbeeld** zijn, waarmee hij zijn stelling $p \to q$ meteen ontkracht. Maar wel de stelling $\neg(p \to q)$ bewees.

2.3.2 Soorten bewijsmethodes voor de stelling $p \leftrightarrow q$

Definitie. *Het bewijs van een stelling $p \leftrightarrow q$ is een opeenvolging van logische argumenten om aan te tonen dat de formule $p \leftrightarrow q$ (óf elke formule die hier logisch equivalent mee is), een tautologie is.*

Als we spreken over de stelling $p \leftrightarrow q$, zeggen we dikwijls dat p de nodige en voldoende voorwaarde is voor q. Dan valt het bewijs van de stelling uiteen in twee delen:

1. De voorwaarde is **voldoende** indien $v(p) = 1$ impliceert dat ook q waar is. We moeten dus aantonen dat $p \to q$ een tautologie is.
2. De voorwaarde is **nodig** indien $v(p) = 0$ impliceert dat ook q niet waar is. Dus hiervoor moeten we aantonen dat $\neg p \to \neg q \equiv q \to p$ een tautologie is.

Een praktijkvoorbeeld waar deze terminologie van pas komt, vind je op blz 76.

Oefening 14

Ga na welke van de onderstaande formules logisch equivalent zijn met $p \to q$. Gebruik een waarheidstabel.

- $q \to p$ (**converse** *van* $p \to q$)
- $\neg p \to \neg q$ (**inverse** *van* $p \to q$)
- $\neg q \to \neg p$ (**contrapositie** *van* $p \to q$)

Oefening 15

Schrijf converse, inverse en contrapositie van volgende uitspraken:

1. *Als het niet regent, ga ik naar zee.*
2. *Als mijn oefeningen af zijn, neem ik pauze.*

Oefening 16

Duid aan welk type van bewijsvoering (direct bewijs, bewijs via contrapositie, bewijs uit het ongerijmde, inductie, gevallenstudie) gebruikt wordt in het bewijs van onderstaande uitspraken. Let op: strikvragen mogelijk.

1. *Het getal* $\sqrt{2}$ *is irrationaal.*
2. $(x + y) > 100 \Rightarrow (x > 50$ *of* $y > 50)$
3. $n \in \mathbb{N} \Rightarrow n^3 - n$ *is even*
4. *De som van 2 volkomen kwadraten van even getallen is geen volkomen kwadraat.*
5. *Het kwadraat van een even getal is even.*
6. *Als het kwadraat van een geheel getal* a *even is, is* a *even.*

2.3.3 Stijlafspraken voor wiskundige bewijsvoeringen

Op blz 14 toonden we aan dat $n^3 < 3^n$ voor $n \geq 4$. Heb je enkel de ongelijkheden genoteerd die ons tot het eindbesluit voerden, dan heb je hoogstwaarschijnlijk later heel wat moeite om de juiste redenering weer op te bouwen. En waar moest er nu $\Rightarrow$ dan wel $\Leftrightarrow$ staan? Zou je dit bewijs echter gepubliceerd vinden in (vak)literatuur, dan zal je een heel andere bladspiegel aantreffen. Lange opsommingen van formules en afleidingen zónder tekst zijn zeldzaam. (Als het straightforward rekenwerk is, worden de tussenstappen trouwens weggelaten, en staat er met een fraai eufemisme "na enig rekenwerk vindt men...".) Meer aandacht gaat naar het waarom van de neergeschreven formules. Zo zal er meestal duidelijk aangegeven worden om welk soort bewijs het gaat (uit het ongerijmde, gevallenstudie, inductie (en waaróp)). Zijn de overgangen tussen de formules niet altijd heel duidelijk, dan wordt dit in korte bewoordingen tussenin duidelijk gemaakt. Zo worden $\Rightarrow$ (daaruit volgt) en $\Leftrightarrow$ (als en slechts als) dikwijls verwoord in plaats van als teken neergeschreven. Let bovendien eens op de zinsbouw in bewijzen: een zin zal nooit met een lettervariabele beginnen. Heb je een punt p en een rechte L, dan schrijf je niet "p ligt niet op L want...", maar "Het punt p ligt niet op de rechte L want...". Onthoud: het cement van de taal is minstens zo belangrijk als de bouwstenen van de formules.

Hoofdstuk 3

Tellen

and Christopher Robin knew that it was enchanted, because every time he tried to count the number of trees he could never tell if it was 63 or 64, even if he tied string around each tree as he counted them. — *A.A.Milne*

In de inleiding was er al sprake van: tellen wordt je met de paplepel ingegoten. Maar tellen en tellen is twee.

In dit hoofdstuk laten we een aantal technieken de revue passeren, die de vraag "hoeveel?" beantwoorden zonder alle mogelijkheden expliciet op te sommen. Zo kunnen we bijvoorbeeld vragen "hoeveel woorden van drie letters bestaan er", of "hoeveel ordeningen van n verschillende elementen bestaan er?". Maar ook de vraag "bestaat er...?" kan soms beantwoord worden zónder een expliciet voorbeeld op te dissen.

3.1 Verzamelingenleer

Onze tellingen zullen steeds over elementen gaan die aan welbepaalde eigenschappen voldoen. Deze elementen behoren dus tot een verzameling bepaald via die eigenschappen, zodat een korte herhaling van enkele begrippen uit de verzamelingenleer hier wel op zijn plaats is.

Een **verzameling** wordt volledig bepaald door zijn elementen. Hetzelfde element kan geen tweemaal in de verzameling zitten, en de elementen van een verzameling zijn (a priori) niet geordend. Twee verzamelingen zijn dus gelijk als ze dezelfde elementen bevatten; bijvoorbeeld $\{1, 2, 3, 1\} = \{3, 2, 1\}$. Voorts gelden volgende notaties, voor verzamelingen A, B, C, A_i en elementen x, y, a, b:

$x \in A$	x is element van A	
$x \notin A$	x is geen element van A	
$A \subseteq B$	A is deelverzameling van B	$(\forall x)(x \in A \to x \in B)$
$A \subset B$	A is strikte deelverzameling van B	$(\forall x)(x \in A \to x \in B)$ $\wedge(\exists y)(y \in B \wedge y \notin A)$
ϕ	ledige verzameling	
$A \cap B$	doorsnede van A en B	$= \{x \mid x \in A \wedge x \in B\}$
$A \cup B$	unie van A en B	$= \{x \mid x \in A \vee x \in B\}$
$A \setminus B$	verschil van A en B	$= \{x \mid x \in A \wedge x \notin B\}$
$\overline{A}$	complement van A tov een verzameling U, met $A \subset U$ (U blijkt meestal uit de contekst)	$= U \setminus A$
$\|A\|$	aantal elementen van A $=$ cardinaliteit van A	
2^A	verzameling van alle deel-verzamelingen van A	
(x, y)	geordend paar van 2 elementen	dus $(a, b) \neq (b, a)$
$A \times B$	Cartesisch product van A en B vb: $\{a, b\} \times \{a, b, c\}$ $= \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c)\}$	$= \{(a, b) \mid a \in A \wedge b \in B\}$
$A_1 \times A_2 \times \ldots \times A_n$	Cartesisch produkt van A_i $(i = 1 \to n)$ $= \Pi_{i=1}^{n} A_i = \Pi A_i$	
A^n	n-voudig Cartesisch produkt van A	$= A \times A \times \ldots \times A$

De deelverzamelingen van een gegeven verzameling vormen een Booleaanse algebra onder de operatoren $\cap$ en $\cup$. We kunnen nagaan dat commutativiteit, associativiteit, distributiviteit en De Morgans wetten van toepassing zijn; eventueel aan de hand van een Venn diagram.

	$A \cap B$	$=$	$B \cap A$	$A \cup B$	$=$	$B \cup A$
	$A \cap (B \cap C)$	$=$	$(A \cap B) \cap C$	$A \cup (B \cup C)$	$=$	$(A \cup B) \cup C$
	$A \cap (B \cup C)$	$=$	$(A \cap B) \cup (A \cap C)$	$A \cup (B \cap C)$	$=$	$(A \cup B) \cap (A \cup C)$
	$A \setminus (B \cap C)$	$=$	$(A \setminus B) \cup (A \setminus C)$	$A \setminus (B \cup C)$	$=$	$(A \setminus B) \cap (A \setminus C)$
is analoog met	$\overline{(B \cap C)}$	$=$	$\overline{B} \cup \overline{C}$	$\overline{(B \cup C)}$	$=$	$\overline{B} \cap \overline{C}$

Twee verzamelingen hebben zelfde cardinaliteit als er een bijectie (1-op-1-relatie) bestaat tussen hun elementen. Als $|A| \in \mathbb{N}$, dan is de verzameling A **eindig**. Een oneindige verzameling is **aftelbaar oneindig** als er een bijectie bestaat met de natuurlijke getallen $\mathbb{N}$. Anders noemen we ze overaftelbaar. Zo zijn $\mathbb{Z}$ én $\mathbb{Q}$ aftelbaar oneindig, maar $\mathbb{R}$ niet (dit laatste wordt aangetoond met het diagonaalbewijs van Cantor). Toch hebben niet alle overaftelbare verzamelingen dezelfde grootte.

Als $A \subset B$ en $|A| = k$, dan noemen we A een **k-deelverzameling** van B. Volgende eigenschappen gelden in verband met de cardinaliteit van (eindige) verzamelingen:

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ |2^A| &= 2^{|A|} \\ |A \times B| &= |A| \cdot |B| \\ |\Pi A_i| &= \Pi |A_i| \end{aligned}$$

Om de tweede gelijkheid te bewijzen, beeld je elk element a_i van A af op 0 dan wel 1, waarbij 0 staat voor '*behoort niet tot deelverzameling*' en 1 voor '*behoort wel tot deelverzameling*'. Voor elke a_i heb je 2 keuzes, voor het geheel van elementen $(a_1, a_2, \ldots a_{|A|})$ heb je er $2^{|A|}$. Met andere woorden er zijn $2^{|A|}$ mogelijke afbeeldingen van $(a_i)_{i=1 \to |A|}$, dus $2^{|A|}$ mogelijke deelverzamelingen. Dit liep even vooruit op paragraaf 3.2.3; zie ook blz 50.

3.2 Telformules

We geven een overzicht van de meest gekende telregels en -formules, afkomstig uit de verzamelingenleer en de combinatoriek — en eentje uit het dierenrijk.

3.2.1 Het ladenprincipe van Dirichlet

In het Engels wordt dit het pigeonhole of duivenhokprincipe genoemd. Laten we het in deze bewoordingen ook formuleren.

Stelling 3.1. *Als er n duivenhokken zijn en meer dan $k \cdot n$ duiven, dan is er minstens één hok waar $k + 1$ of meer duiven in zitten.*

Bewijs Bewijs uit het ongerijmde. Stel dat de premissen uit de stelling waar zijn, maar dat er geen enkel hok is met meer dan k duiven. Dus zijn er maximaal $k \cdot n$ duiven, in contradictie met de premisse over het aantal duiven. □

Dit eenvoudige principe is niet zozeer een telformule (geeft geen antwoord op de vraag 'hoeveel'), maar een manier om het bestaan van iets te bewijzen. Dikwijls gaat het hierbij om een koppel elementen met een speciale eigenschap dat gezocht wordt. Voor niet-triviale toepassingen verwijzen we naar de eerste oefeningen op blz 52.

3.2.2 Somprincipe

Het aantal manieren om een element te kiezen uit 2 disjuncte eindige verzamelingen is de som van de cardinaliteiten van de verzamelingen. Formeel:

$$|A \cup B| = |A| + |B| \text{ voor } A \text{ en } B \text{ disjunct}$$

Voorbeeld: als het eerste teken van een nummerplaat een letter óf cijfer is, dan heb je voor die positie 26+10=36 keuzes (waarbij 'nul' en de letter 'O' voor het gemak even verschillend ondersteld werden). Via inductie kunnen we de algemene vorm bewijzen van het somprincipe: $|A_1 \cup A_2 \cup \ldots \cup A_k| = \sum_{i=2}^{k} |A_i|$ met A_i twee aan twee disjuncte eindige verzamelingen.

3.2.3 Produktprincipe

Het aantal manieren om een geordend koppel te kiezen is het aantal manieren om het eerste element te kiezen maal het aantal manieren om het tweede element te kiezen. Formeel:

$$|A \times B| = |A| \cdot |B| \text{ voor } A \text{ en } B \text{ eindig}$$

Voorbeeld: het aantal nummerplaten van 4 tekens waarbij het 1^e teken letter óf cijfer is, het 2^e en 3^e teken een letter en het 4^e een cijfer, is $36 \cdot 26 \cdot 26 \cdot 10$.

3.2.4 Inclusie-exclusie principe

Een uitbreiding van het somprincipe voor niet-disjuncte verzamelingen is het eenvoudige inclusie-exclusieprincipe. In woorden: als A en B twee eindige verzamelingen zijn, is het cardinaalgetal van hun unie gelijk aan de som van de cardinaalgetallen van A en B afzonderlijk, waarvan het cardinaalgetal van hun doorsnede wordt afgetrokken.

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Het veralgemeend inclusie-exclusieprincipe voor meerdere verzamelingen kan (o.a.) bewezen worden aan de hand van een telformule uit de combinatoriek (zie verder). We geven het hieronder voor vier verzamelingen A_1, A_2, A_3, A_4.

$$\begin{aligned} |A_1 \cup A_2 \cup A_3 \cup A_4| \;=\; & |A_1| + |A_2| + |A_3| + |A_4| \\ & -|A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| \\ & -|A_2 \cap A_3| - |A_2 \cap A_4| - |A_3 \cap A_4| \\ & +|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| \\ & +|A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\ & -|A_1 \cap A_2 \cap A_3 \cap A_4| \end{aligned}$$

3.2.5 Permutaties

Een **permutatie** van een eindige verzameling S is een geordende rij van alle elementen van S, waarbij elk element juist één maal voorkomt. Er zijn $n!$ permutaties van een verzameling van n elementen: voor het eerste element heb je n keuzes, voor het tweede nog $n-1$ enz.

$$P_n = n!$$

3.2.6 Vier formules uit de combinatoriek

Hierboven stond al een formule uit de combinatoriek. In deze tak van de wiskunde stelt men formules op om, gegeven een verzameling elementen, te berekenen hoeveel verschillende structuren opgebouwd kunnen worden uit deze elementen. Voorbeeld: gegeven $\{1, 2, 3, 4\}$, hoeveel getallen van 6 cijfers kan je hiermee vormen? Hierbij dient dan wel aangegeven te worden hóe een structuur mag opgebouwd zijn (herhaling, geen herhaling) en wanneer twee structuren als gelijk beschouwd worden (geordend, ongeordend). Deze twee eigenschappen van de opgebouwde structuren zullen we telkens terugvinden in de beschrijving van het probleem en de afgeleide formules.

Voor de volgende vier telsituaties spelen we met de lotto — maar passen de spelregels wat aan. Er zitten n genummerde ballen in de trommel, en we halen er k uit.

A Stel dat we een getrokken bal *niet terugsteken* vóór we de volgende trekken.

- Het aantal mogelijke uitkomsten van de trekking, als de volgorde waarin ze getrokken worden van belang is, is $\underbrace{n(n-1)\dots(n-k+2)\cdot(n-k+1)}_{k \text{ keer}} = \frac{n!}{(n-k)!}$. We noemen een geordende rij van k elementen van een (eindige) verzameling waarbij elk element maximaal één maal voorkomt een **k-permutatie** of variatie van S. We noteren het aantal **variaties van k uit n** als
$$V_n^k = \frac{n!}{(n-k)!}$$

- Als de volgorde van trekken geen belang heeft, zitten er tussen de $\frac{n!}{(n-k)!}$ k-permutaties die we daarnet telden, telkens een aantal equivalente trekkingen. Gezien de trekking $a_1a_2a_3a_4$ nu gelijk wordt ondersteld aan de trekkingen $a_2a_1a_3a_4$, $a_2a_3a_4a_1$, ... hebben we dus telkens $k!$ equivalente trekkingen (met $k!$ het aantal permutaties van k elementen). Het aantal mogelijke uitkomsten van de trekking zonder teruglegging en waar volgorde geen belang heeft, is dus $\frac{n!}{(n-k)!k!}$. Elke trekking komt hier duidelijk overeen met een **k-deelverzameling** van S, ook wel k-combinatie genoemd, of **combinatie van k elementen uit n**. We schrijven
$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

B Stel dat we een getrokken bal *wel terugsteken* voor we de volgende trekken.

- Als de volgorde van trekken belang heeft, hebben we in totaal $\overbrace{n \cdot n \cdot \ldots \cdot n}^{k \text{ keer}} = n^k$ mogelijke uitkomsten. Een geordende rij van k elementen uit S (met $|S| = n$) waarbij elk element meerdere malen mag voorkomen, noemen we een **herhalingsvariatie van k uit n**. Merk op: hier hoeft k niet per se kleiner te zijn dan n. We schrijven
$$\overline{V}_n^k = n^k$$

- Als de volgorde van trekken geen belang heeft, spreken we van een **herhalingscombinatie**. Het aantal herhalingscombinaties van k elementen uit n is niet onmiddellijk af te leiden uit vorige berekening. Immers, de trekking 1 1 1 1 2 heeft 5 equivalenten (zichzelf inbegrepen), terwijl de trekking 1 2 3 4 5 er 5! heeft. Het is dus niet zo dat je het aantal herhalingsvariaties door een constante kan delen, om aan het aantal herhalingscombinaties te komen.
  Maar stellen we ons probleem anders voor: trekken we uit $\{1, 2, 3, 4, 5, 6\}$ *met* terugleggen, en is de volgorde *niet* van belang, dan volstaat het om per element aan te duiden hoe dikwijls dat element voorkomt — een frequentietabel. We schetsen deze frequentietabel (enkel de verticale tussenschotten volstaan), en per getrokken element zetten we een bolletje in het overeenstemmende 'hokje'. De trekkingen 2 5 2 4 4 4 6 en 2 2 5 6 4 4 4 bijvoorbeeld komen overeen met

  | • • | | • • • | • | •

  (en de verdeling | | | | | ••••••• komt eenduidig overeen met ...). Elke opeenvolging van k bolletjes en $n-1$ stokjes komt dus overeen met één herhalingscombinatie. Het aantal verschillende schetsen dat we zo kunnen maken, wordt gegeven door het aantal manieren waarop je $n-1$ van de $k+n-1$ plaatsen kan kiezen waarop je een tussenschot zet. De volgorde waarin je de tussenschotten zet speelt natuurlijk geen rol, maar je mag geen twee tussenschotten op één plaatsje zetten. Het gaat hier dus om een $(n-1)$-combinatie uit $(k+n-1)$ elementen.[1] Gevolg: er zijn

  $$\overline{\binom{n}{k}} = \binom{k+n-1}{n-1} = \binom{k+n-1}{k}$$

  herhalingscombinaties van k elementen uit n.

Zetten we de vier voorgaande tellingen in een schema, dan hebben we

	zonder terugleggen	met terugleggen
ongeordend	$\binom{n}{k}$	$\overline{\binom{n}{k}} = \binom{n+k-1}{k}$
geordend	$n(n-1)\dots(n-k+1)$	n^k

3.2.7 Toepassingen op combinatieleer

We sommen hier een aantal toepassingen op, met verwijzingen.

- binomiale kansverdeling (zie bijlage)
- aantal deelverzamelingen van een verzameling (blz 47)

[1] Heb je deze zin écht begrepen? Dit is cruciaal in het bewijs, en het kan geen kwaad om – voor je verder lee$\binom{s}{r}$t – nog eens aan jezelf uit te leggen waarom deze uitspraak waar is. Wat zijn trouwens die 'elementen' waarvan sprake?

- binomium van Newton (blz 55)
- bewijs van veralgemeend inclusie/exclusie-principe
- wanordes

3.2.8 Dubbele telling

Een laatste telprincipe dat we hier behandelen is dat van de dubbele telling. Hoewel niet algemeen gekend, is het een principe dat zeer dikwijls gebruikt wordt in de discrete variant van de analytische meetkunde: de eindige meetkunde of incidentiemeetkunde. Zowel grafentheorie (cursus *Algoritmen*) als codeertheorie (cursus *Beveiliging*) sluit zeer nauw aan bij de theorie van de incidentiemeetkunde. Vandaar dat dit telprincipe in een cursus voor informatici opduikt. We illustreren het principe aan de hand van een voorbeeld.

Voorbeeld

> Gegeven een stad met 70 straten, in elke straat precies 30 huizen, en elk huis op kruispunt van precies 3 straten (het huis wordt dan ondersteld in elk van deze straten te liggen). Hoeveel huizen telt deze imaginaire stad?
>
> We tellen op 2 manieren het aantal koppels (h, s) waarbij h een huis is dat gelegen is in straat s. $\boxed{1}$ In elke straat staan er 30 huizen, dus een gegeven s_i komt voor in 30 koppels (h, s_i). In totaal zijn er 70 straten s_i. Dit geeft $30 \cdot 70$ koppels in totaal. $\boxed{2}$ Voor elk huis h_j zijn er 3 straten s, dus elk huis h_j komt voor in 3 koppels (h_j, s). Het totaal aantal huizen h_j is de onbekende factor, en noemen we x. Dit geeft $3 \cdot x$ koppels.
>
> Hieruit volgt dat $x = 700$: er zijn 700 huizen in deze stad.

Omdat het bij grotere vraagstukken niet altijd duidelijk is wélke koppels je moet tellen (vooral als er meerdere soorten elementen in het spel zijn), maken we soms een schets van de situatie. We tekenen elke elementenverzameling (huizen respectievelijk straten), uiteraard disjunct. Een koppel (h, s) wordt dan voorgesteld door een pijl of verbinding tussen (een element van) de eerste verzameling en (een element van) de tweede verzameling. We tellen de koppels (h, s) door de verbindingen op twee plaatsen te tellen: waar ze vertrekken én waar ze toekomen. Dit aantal moet dan uiteraard gelijk zijn. $\boxed{1}$ Daartoe fixeren we eerst een element uit de eerste verzameling, en duiden op een vertrekkende pijl aan hoeveel verbindingen er (min/max/exact) vanuit dat ene element vertrekken. Dit vermenigvuldigen we met het aantal elementen in de eerste verzameling. $\boxed{2}$ In de tweede verzameling fixeren we ook een element, en duiden op een toekomende pijl aan hoeveel verbindingen er (min/max/exact) in dit element toekomen. Dit wordt vermenigvuldigd met het aantal elementen in de tweede verzameling. Uit gelijkstelling van beide produkten volgt dan de gevraagde (on)gelijkheid of het onbekende aantal.

3.3 Oefeningen

Waarschuwing
Het is niet omdat er 4 basisformules bestaan in de combinatoriek, dat het in een oefening volstaat om één van die formules uit de kast te trekken. Het is eerder aangeraden om diezelfde redeneringen te volgen die tot de formules geleid hebben, nu toegepast op de nieuwe situatie. Vind je dit moeilijk? Maak (doordacht!) gebruik van de hints bij de oefeningen, tot je het systeem doorhebt.

Soms is het verleidelijk om bij een teloefening (zoals oef 17) over te schakelen op kansrekening. In plaats van dan effectief te tellen hoeveel elementen er aan een bepaalde voorwaarde voldoen (dit impliceert gehele getallen), zou je kunnen uitgaan van het totale aantal elementen, en vermenigvuldigen met de kans (< 1) dat de voorwaarde zich voordoet (dit impliceert breuken). Is die kans echter afhankelijk van meerdere / onbekende factoren, dan zal deze methode falen. Moraal: toch maar tellen in $\mathbb{N}$...

Oefening 1

Hoeveel mensen moet je kiezen uit 15 getrouwde stellen, om er zeker van te zijn dat je zeker 3 koppels gevonden hebt?

Oefening 2

Hoeveel verschillende gehele getallen moet je kiezen om er zeker 10 te hebben die tot dezelfde congruentieklasse modulo 7 behoren?

Oefening 3

Gegeven een gelijkzijdige driehoek met zijde 1, en vijf punten die binnen deze driehoek gelegen zijn. Toon aan dat de afstand tussen één van de puntenparen niet groter is dan $\frac{1}{2}$.

Oefening 4

(bonus) In elke groep mensen zijn er steeds 2 mensen te vinden die evenveel vrienden hebben — als de vriendschappen wederkerig zijn. Toon aan met het ladenprincipe van Dirichlet.

Oefening 5

Zes vrienden gaan samen pingpongen. Hoeveel verschillende partijen enkelspel en dubbelspel kunnen ze spelen?

Oefening 6

Gegeven vier punten in een vlak, waarvan geen drie collineair. Men tekent alle rechten bepaald door die vier punten. Hoeveel nieuwe snijpunten worden door deze rechten bepaald? Neem aan dat geen twee van de rechten evenwijdig zijn. Stel daarna een veralgemening van de formule voor, voor n gegeven punten.

Oefening 7

Een codewoord bestaat uit negen verschillende tekens. Eerst 4 hoofdletters, daarna 3 kleine letters, tenslotte 2 cijfers. Hoeveel mogelijke codewoorden zijn er?

Oefening 8

Men vormt alle mogelijke getallen van drie cijfers met de cijfers 1, 2, 3, 4, 5 *en rangschikt deze getallen in stijgende volgorde.*

1. *Hoeveel dergelijke getallen zijn er?*
2. *Wat is het volgnummer van 251, 333 en 454?*
3. *Welk getal staat op de 21e plaats?*

Oefening 9

Op hoeveel manieren kan men 12 verschillende knikkers verdelen over 3 jongens, als één ervan 6 knikkers moet krijgen, een andere 4 en de laatste 2?
En als de eerste jongen er minimum 6 moet krijgen, de tweede maximum 5 maar niet minder dan de laatste, en de laatste niet zonder naar huis wil?

Oefening 10

Gegeven 10 dames en 10 heren. De heren krijgen een nummer van 1 tot 10 toegewezen, de dames loten hun nummer van 1 tot 10 uit. Op hoeveel verschillende manieren kan men op deze manier 10 koppels bekomen?

Oefening 11

Hoeveel verschillende getallen van 4 verschillende cijfers zitten er tussen 1500 en 4000?

Oefening 12

Kan je de getallen $1, 2, \ldots, 12$ *in cirkelvorm schrijven, zodat de som van 5 opeenvolgende getallen nooit groter is dan 32?*

Oefening 13

Je hebt 4 rode rozenstruiken, 3 roze en 5 witte. Op hoeveel manieren kan je deze in een rij aanplanten? (Struiken van dezelfde kleur kan je onderling niet onderscheiden.)

Oefening 14

Hoeveel anagrammen bestaan er van het woord

1. *ANAGRAM*
2. *BANANENBOOT*
3. *HOTTENTOTTENTENTENTENTOONSTELLING*

Oefening 15

Uit hoeveel stenen bestaat een dominospel? Elke dominosteen is verdeeld in 2 helften waarop 0 tot 6 stippen kunnen staan. Er zijn geen gelijke stenen, en elke combinatie komt eenmaal voor.

Oefening 16

Gegeven 5 wolven, 10 schapen en 4 genummerde kooien. Op hoeveel manieren kan men de dieren in de kooien stoppen, zodanig dat wolven en schapen niet samen zitten? De wolven zijn van elkaar niet te onderscheiden, de schapen ook niet.

Oefening 17

Met de cijfers 0 tot 9 worden getallen bestaande uit 5 verschillende cijfers gevormd. Opgelet: de opeenvolging 01234 *geldt niet als getal van 5 verschillende cijfers; de opeenvolging* 12340 *wél.*

1. *Hoeveel van die getallen bestaan er?*
2. *Hoeveel van deze getallen bevatten het cijfer 6?*
3. *Hoeveel van deze getallen bevatten de cijfers 0 en 7?*
4. *Hoeveel van deze getallen zijn even en bevatten het cijfer 5?*

Oefening 18

Stel dat in de imaginaire stad waarvan sprake op blz 51, elk huis op het kruispunt van maximum *3 straten ligt. Hoeveel huizen zijn er dan?*

Oefening 19

Gegeven een eindige structuur van punten, rechten en vlakken. Er is een symmetrische incidentie-relatie I gedefinieerd tussen punten en rechten, tussen punten en vlakken en tussen rechten en vlakken. We zeggen dat een punt p op een rechte R ligt, en de rechte R door het punt p gaat, als $I(p, R)$. Een punt p ligt in een vlak π, en het vlak π bevat het punt p als $I(p, \pi)$. Een rechte R ligt in een vlak π en het vlak π bevat de rechte R, als $I(R, \pi)$. Voorts geldt $I(p, R) \wedge I(R, \pi) \rightarrow I(p, \pi)$. We weten volgende zaken van deze structuur:

- *Er zijn $(q^2 + 1)(q^2 + q + 1)$ rechten.*
- *Er zijn $(q^3 + q^2 + q + 1)$ punten.*
- *Elk punt is incident met evenveel rechten.*
- *Elk punt is incident met $(q^2 + q + 1)$ vlakken.*
- *Elke rechte is incident met evenveel punten als vlakken, en dit aantal is voor elke rechte gelijk.*
- *Elk vlak bevat evenveel rechten als punten, nl. $(q^2 + q + 1)$.*

Gevraagd: hoeveel rechten gaan er door 1 punt, hoeveel punten liggen er op 1 rechte?

Hoofdstuk 4

Voortbrengende functies en recurrente betrekkingen

In vorig hoofdstuk zagen we de 4 hoofdformules van de combinatoriek, opgedeeld volgens het schema zoals op blz 50. Dit schema dekt echter niet alle mogelijkheden. Stel bijvoorbeeld dat je 10 kinderen een stuk fruit wil geven als je 4 peren hebt, 2 kiwi's en zoveel appels als je wil (gezien je in de boomgaard staat). Gevraagd is: op hoeveel verschillende manieren kan je dit doen? Dit keuzeprobleem valt niet onder de noemer '*met terugleggen*' (rechterkolom), want na 4 stuks ben je uitverkocht wat peren betreft. Het valt echter ook niet onder de noemer '*zonder terugleggen*' (linkerkolom). Daarvoor zou je immers de verzameling waaruit je mag kiezen moeten gelijkstellen aan $\{\text{peer}_1,\text{peer}_2,\text{peer}_3,\text{peer}_4,\text{kiwi}_1,\text{kiwi}_2,\ \text{appel}_1,...,\text{appel}_{10}\}$. Uiteraard komt de keuze '*Jan krijgt peer*$_1$*, Piet krijgt peer*$_2$' op hetzelfde neer als de keuze '*Jan krijgt peer*$_2$*, Piet krijgt peer*$_1$'. Zou je dan kunnen opperen dat het hier om een ongeordende keuze uit 16 elementen zonder terugleggen gaat? Neen, want als Jan een peer krijgt en Piet een appel, doet de volgorde er wél toe. Met andere woorden: dit probleem is niet oplosbaar aan de hand van de methodes die in hoofdstuk 3 aan bod kwamen. In hoofdstuk 3 heb je immers ofwel allemaal unieke (= verschillende) elementen waaruit je je keuze samenstelt, ofwel verschillende soorten elementen waarbij elke soort overvloedig vertegenwoordigd is. Telproblemen echter waarbij herhaling (of teruglegging) *deels* mogelijk is, hebben een eigen oplossingsmethode nodig. Voor we deze methode uitbouwen, maken we een zijstap naar het binomium van Newton.

4.1 Binomium van Newton

Tot zijn essentie herleid: het binomium van Newton is een wiskundige formule die de macht van een som omzet in een som van machten. Meer precies: de macht van de som van twee grootheden wordt uitgedrukt in een som van termen waarin de machten van de grootheden afzonderlijk voorkomen. In formulevorm:

$$(x+y)^n = \sum_{k=0}^{n} a_{n,k} x^k y^{n-k}$$

waarbij n een natuurlijk getal is, en $a_{n,0}, a_{n,1}, ..., a_{n,n}$ de binomiaalcoëfficiënten zijn die je kan aflezen uit onderstaande driehoek:

$a_{0,0}$	1
$a_{1,0}$ $a_{1,1}$	1 1
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$	1 2 1
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$	1 3 3 1
$a_{4,0}$ $a_{4,1}$ $a_{4,2}$ $a_{4,3}$ $a_{4,4}$	1 4 6 4 1

Is er echter geen andere manier om aan deze binomiaalcoëfficiënten te raken dan bovenstaande driehoek op te stellen? Om een antwoord te vinden, volstaat het een voorbeeld uit te werken voor $n = 5$, en daaruit een verband met de combinatoriek af te leiden.

$$(x+y)^5 = (x+y)(x+y)(x+y)(x+y)(x+y)$$

Om dit product te ontwikkelen, zal je volgens het principe van de associativiteit uit elke factor telkens één term moeten kiezen (dus x of y), en deze 5 termen vermenigvuldigen met elkaar. Daarna tel je al deze grootheden bij elkaar op. Hoe dikwijls zal nu x^2y^3 voorkomen in de uitwerking (of ontwikkeling) van dit product? Telkens je uit 2 van de 5 factoren de term x kiest (en uit de overige factoren de term y), komt x^2y^3 één keer voor in de ontwikkeling. Je moet dus 2 factoren van de 5 aanduiden waaruit je x kiest. Dit kan op $\binom{5}{2}$ manieren. Algemeen: de coëfficiënt van $x^k y^{n-k}$ in de ontwikkeling van $(x+y)^n$ is het aantal manieren om in het product

$$\underbrace{(x+y) \quad (x+y) \quad \dots \quad (x+y)}_{n \text{ keer}}$$

precies k van de n factoren aan te duiden waar je x uit kiest in plaats van y. Dit komt overeen met het aantal combinaties van k elementen uit n elementen, dus $\binom{n}{k}$. Daaruit halen we de uiteindelijke vorm van het binomium van Newton:

$$\boxed{(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}}$$

Voor de bepaling van de binomiaalcoëfficiënten $a_{n,k}$ hoeven we dus niet de hele driehoek van Pascal[1] op te stellen (wat neerkomt op een recursieve bepalingsmethode), maar hebben we de rechtstreekse formule $a_{n,k} = \binom{n}{k}$. In het tweede deel van dit hoofdstuk komen we terug op het verband tussen recursieve versus rechtstreekse bepaling van een gezochte grootheid.

4.2 Tellingen aan de hand van voortbrengende functies

Terug naar ons telprobleem. We vereenvoudigen de opgave eerst; de fruitmand bevat nu 1 appel, 1 banaan en 1 citroen. Op hoeveel manieren kan je 2 stuks fruit kiezen? We moeten

[1] De formule $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(k+1)}{k!}$ en de rangschikking van binomiaalcoëfficiënten in een driehoek worden vaak toegeschreven aan Blaise Pascal omdat die ze in de 17e eeuw beschreef en de naam *binomium van Newton* (van het Latijnse *tweeterm*) gaf. De formule was bij Chinese wiskundigen echter lang daarvoor al bekend.

uit elke factor van volgend '*product*' dus één term kiezen (nl. wel of geen stuk fruit van die soort), en ervoor zorgen dat we in totaal 2 stukken fruit hebben.

(0 appels of 1 appel) (0 bananen of 1 banaan) (0 citroenen of 1 citroen)

Herschrijven we dit '*product*' als

$$\begin{array}{rl} & (a^0+a^1)\ \ (b^0+b^1)\ \ (c^0+c^1) \\ = & (1\ \ +a\ )\ \ (1\ \ +b\ )\ \ (1\ \ +c\ ) \end{array}$$

waarbij $a^0 = 1$ staat voor 0 appels en a^1 staat voor één appel. Juist 2 stukken fruit kiezen, komt dus overeen met precies 2 factoren aanduiden waaruit je een eerste graad kiest in plaats van een nulde graad. De truc bestaat er nu in om in de formule geen onderscheid te maken tussen a, b of c (nl. appel, banaan of citroen), maar om gewoon van 'fruit' te spreken.

$$\underbrace{(1+x)}_{appels}\ \underbrace{(1+x)}_{bananen}\ \underbrace{(1+x)}_{citroenen}$$

Nu komt 2 stuks fruit kiezen overeen met precies 2 factoren aanduiden waaruit je de term x kiest in plaats van de term 1. Het aantal manieren om 2 stuks te kiezen wordt dan de coëfficiënt van x^2 in de ontwikkeling van $(1+x)^3$. Gezien $(1+x)^3 = 1+3x+3x^2+x^3$, is het antwoord op de vraag 3. Dit hadden we uiteraard ook meteen kunnen berekenen uit $\binom{3}{2} = 3$, maar enkel en alleen omdat het probleem te herleiden was tot de linkerkolom van het schema op blz 50. Richten we ons nu terug op een niet-triviale opgave. Stel dat de fruitmand 2 appels, 1 banaan en 1 citroen bevat. Dan komen we uit op volgende mogelijkheden:

(0 appels of 1 appel of 2 appels) (0 bananen of 1 banaan) (0 citroenen of 1 citroen)

De keuze voor 0, 1 of 2 appels sluiten elkaar uit: ze worden dus volgens het somprincipe behandeld. De keuze voor enerzijds een (aantal) appel(s) en anderzijds wel of geen banaan sluiten elkaar niet uit, en zullen dus volgens het productprincipe behandeld worden. Zo komen we tot

$$\begin{array}{rl} & (a^0+a^1+a^2)\ \ (b^0+b^1)\ \ (c^0+c^1) \\ \text{of nog:} & \underbrace{(1\ \ +x\ \ +x^2)}_{appels}\ \ \underbrace{(1\ \ +x\ )}_{bananen}\ \ \underbrace{(1\ \ +x\ )}_{citroenen} \end{array}$$

Twee stukken fruit kiezen, komt nu overeen met uit elke factor een $1, x$ of x^2 kiezen — tot de som van de gekozen machten 2 is. Het aantal mogelijke manieren om x^2 $(= x^0 \cdot x^1 \cdot x^1 = x^1 \cdot x^0 \cdot x^1 = \ldots)$ te bekomen, wordt gegeven door de coëfficiënt van x^2 in de ontwikkeling van de gegeven uitdrukking. Gezien

$$(1+x+x^2)(1+x)(1+x) = 1+3x+4x^2+3x^3+x^4,$$

zien we dat het antwoord op de vraag 4 is.

appels	2	1	1	0
banaan	0	1	0	1
citroen	0	0	1	1

Merk nogmaals op: twee elkaar uitsluitende keuzes (0, dan wel 1 of 2 stukken van dezelfde fruitsoort) komen als termen voor in dezelfde factor, twee verschillende fruitsoorten steken we in aparte factoren.

Definitie. *De functie* $(1+x+x^2)(1+x)(1+x) = 1+3x+4x^2+3x^3+x^4$ *noemen we de* **genererende functie** *voor de oplossingen op de vraag* 'op hoeveel manieren kan je k stukken fruit kiezen uit 2 appels, 1 banaan en 1 citroen?'. *Uit deze functie valt immers voor elke k het antwoord onmiddellijk af te lezen!*

Voorbeeld

Stel dat iemand r stuks gebak wil bestellen bij de bakker, die echter nog maar 3 rijsttaarten, 2 fruittaarten en 4 appelcakes heeft. Op hoeveel verschillende manieren kan dit gebeuren?

Het aantal manieren waarop dit kan gebeuren noemen we a_r. We vragen dus de waarde van a_r voor elke mogelijke r. (Uiteraard zal r niet groter zijn dan $3+2+4$, anders is het antwoord $a_r = 0$.) De functie waaruit we het antwoord kunnen aflezen, genaamd de genererende functie van de rij $a_0, a_1, a_2, ...$, kunnen we opstellen analoog aan de vorige situaties:

$$\underbrace{(1+x+x^2+x^3)}_{rijsttaart}\underbrace{(1+x+x^2)}_{fruittaart}\underbrace{(1+x+x^2+x^3+x^4)}_{appelcake}$$

omdat we keuze hebben uit 0 tot 3 rijsttaarten, 0 tot 2 fruittaarten, en 0 tot 4 appelcakes — voor een totaal van r stuks. Uitgewerkt geeft dit

$$1+3x+6x^2+9x^3+11x^4+11x^5+9x^6+6x^7+3x^8+x^9.$$

Dus zijn er 6 manieren om 7 taarten te kiezen uit het aanbod:

rijst	3	3	3	2	2	1
fruit	2	1	0	2	1	2
appel	2	3	4	3	4	4

of algemeen: het aantal manieren a_r om r stuks gebak te kiezen, lees je af uit bovenstaande veelterm; a_r is gelijk aan de coëfficiënt van x^r.

Voorbeeld

Stel dat de appelcakes enkel per 2 verkocht worden, welke mogelijkheden heb je dan? De genererende functie wordt nu

$$\begin{aligned} & (1+x+x^2+x^3)(1+x+x^2)(1+x^2+x^4) \\ = \; & 1+2x+4x^2+5x^3+6x^4+6x^5+5x^6+4x^7+2x^8+x^9 \end{aligned}$$

Er zijn deze keer 4 manieren om 7 stuks gebak uit te kiezen (duid deze aan in de tabel van vorig voorbeeld).

Het rekenwerk in bovenstaande oefeningen was nog makkelijk uit te voeren. Er zijn echter problemen denkbaar, waarbij het rekenwerk wat uit de hand loopt. Zo heb je voor de uitwerking van $(1+x+x^2+x^3)^4$ toch al snel 18 (lange) regels nodig. Er zijn ook problemen

waarbij één of meerdere factoren in principe oneindig zijn, óf waar een antwoord wordt gevraagd in functie van gegeven parameters. Voorbeeld: op hoeveel manieren kan je n mensen iets te drinken geven, als je de keuze hebt uit f glazen fruitsap, b flesjes bier en (zeeeeeer veel) kraantjeswater? Wil je hierop een adequaat antwoord geven, dan is het handig om de gepaste terminologie te gebruiken. Daarom bespreken we in de volgende paragraaf het begrip 'formele machtreeks'.

4.3 Formele machtreeksen en rekenregels

Een **formele machtreeks** is een uitdrukking van de vorm

$$\sum_{k=0}^{\infty} a_k x^k$$

waarbij de getallen $a_k (k \in \mathbb{N})$ tot een bepaalde getallenverzameling behoren (meestal $\mathbb{Z}$, $\mathbb{Q}$ of deelverzameling hiervan), en waarbij x (bij uitbreiding: elke x^i) als symbool te interpreteren is, en níet staat voor één of ander getal uit een getallenverzameling. We moeten ons dus ook niet bekommeren om de convergentie van deze machtreeks.

Bij elke formele machtreeks hoort een rij getallen $(a_k)_{k\in\mathbb{N}} = (a_0, a_1, \ldots)$, en elke rij getallen bepaalt een formele machtreeks. Merk op: elke veelterm $p(x) = \sum_{k=0}^{\mathbf{n}} a_k x^k$ kan als formele machtreeks geschreven worden, mits de afspraak dat $a_m = 0$ voor $m > n$.

Twee machtreeksen zijn gelijk, indien hun getallenrijen $(a_k)_{k\in\mathbb{N}}$ gelijk zijn.

De **rekenregels** voor formele machtreeksen zijn nagenoeg dezelfde als deze voor de veeltermen. Som en produkt kunnen we als volgt schrijven:

$$\begin{array}{rcl} \left(\sum_{k=0}^{\infty} a_k x^k\right) + \left(\sum_{k=0}^{\infty} b_k x^k\right) & = & \sum_{k=0}^{\infty} (a_k + b_k) x^k \\ \left(\sum_{k=0}^{\infty} a_k x^k\right) \cdot \left(\sum_{k=0}^{\infty} b_k x^k\right) & = & \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k \end{array}$$

Formele machtreeksen gehoorzamen dus dezelfde algebraïsche wetten als veeltermen: associativiteit, commutativiteit, distributiviteit van optelling t.o.v. vermenigvuldiging. De eenheid voor de optelling is de formele machtreeks $0 = \sum_{k=0}^{\infty} 0 \cdot x^k$, de eenheid voor de vermenigvuldiging is de formele machtreeks $1 = 1 + \sum_{k=1}^{\infty} 0 \cdot x^k$. De inverse formele machtreeks voor de optelling van de machtreeks $\sum_{k=0}^{\infty} a_k x^k$ is de machtreeks $\sum_{k=0}^{\infty} (-a_k) x^k$. Ook de inverse formele machtreeks voor de vermenigvuldiging bestaat voor elke gegeven formele machtreeks met constante term, op voorwaarde dat die constante term een invers heeft voor de vermenigvuldiging.

Stelling 4.1. *Stel dat $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$. Dan bestaat er een unieke formele machtreeks $g(x)$ zodat $f(x)g(x) = 1$, op voorwaarde dat a_0^{-1} bestaat.*

Bewijs We zoeken een formele machtreeks $g(x) = \sum_{k=0}^{\infty} b_k x^k$ zodat

$$\begin{array}{rcl} f(x)g(x) & = & (a_0 + a_1 x + a_2 x^2 + \ldots)(b_0 + b_1 x + b_2 x^2 + \ldots) \\ & = & a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \ldots \\ & = & 1 \end{array}$$

Dit leidt tot volgende vergelijkingen:

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ &\vdots \end{aligned}$$

De eerste vergelijking is waar als en slechts als $b_0 = a_0^{-1}$, en a_0^{-1} bestaat gezien de onderstelling. Substitueren we deze waarde in de tweede vergelijking, dan is b_1 uniek bepaald. Zo verdergaand, kunnen we elke b_i uniek bepalen. Dus is $g(x) = \sum_{k=0}^{\infty} b_k x^k$ uniek bepaald. □

Het bestaan van een unieke inverse $g^{-1}(x)$ voor elke formele machtreeks $g(x)$ impliceert ook het bestaan van een uniek quotiënt $h(x) = f(x)/g(x) = f(x) \cdot g^{-1}(x)$ voor elke formele machtreeks $f(x)$ en $g(x) = \sum_{k=0}^{\infty} a_k x^k$, indien a_0^{-1} bestaat.

4.4 Voortbrengende functies

Gegeven een uitdrukking $g(x)$ zodat $g(x) = \sum_{k=0}^{\infty} a_k x^k$, dan noemen we de formele machtreeks $\sum_{k=0}^{\infty} a_k x^k$ de **ontwikkeling** van $g(x)$.

Merk op: de uitdrukking $g(x)$ zal dus niet meteen een $\sum$-teken in haar definitie hebben. Het is pas na omvorming (=ontwikkeling), dat er een $\sum$-teken verschijnt.

Gegeven een rij $(a_k)_{k\in\mathbb{N}} = (a_0, a_1, \ldots)$. Elke uitdrukking $g(x)$ wiens ontwikkeling gelijk is aan de formele machtreeks $\sum_{k=0}^{\infty} a_k x^k$, wordt een **voortbrengende** of **genererende functie** van de rij (a_k) genoemd.

Deze voortbrengende functie zal in notatie dikwijls veel korter zijn dan de formele machtreeks, en aldus makkelijker hanteerbaar bij rekenwerk. Daarom is het handig om snel te kunnen overgaan van formele machtreeks op voortbrengende functie, én omgekeerd. De volgende 4 formules vormen de basis van waaruit verdere omzettingen af te leiden zijn.

Stelling 4.2.

voortbrengende functie	*tussen-vorm*	*formele machtreeks*
$1+x$		$= \sum_{k=0}^{\infty} a_k x^k, \quad a_0 = a_1 = 1, a_k = 0 (k > 1)$
$\frac{1}{1-x}$		$= \sum_{k=0}^{\infty} x^k$
$(1+x)^n$		$= \sum_{k=0}^{\infty} \binom{n}{k} x^k$
$\left(\frac{1}{1-x}\right)^n$	$= \left(\sum_{k=0}^{\infty} x^k\right)^n$	$= \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k$

Bewijs

1. De eerste gelijkheid is triviaal, maar werd uit symmetrie-overwegingen toegevoegd.

2. We berekenen het product van de noemer uit het linkerlid, en het rechterlid.

$$(1-x)\left(\sum_{k=0}^{\infty} x^k\right) = \sum_{k=0}^{\infty} x^k - \sum_{k=0}^{\infty} x^{k+1} = \sum_{k=0}^{\infty} x^k - \sum_{k=1}^{\infty} x^k = 1$$

   Gezien x een onbepaalde variabele is (en convergentie-onderzoek niet aan de orde is), volgt de gelijkheid na overbrenging van de factor $(1-x)$.

3. Uit het binomium van Newton. De coëfficiënt van x^k in de ontwikkeling van $(1+x)^n$ is het aantal manieren om uit n factoren precies k factoren aan te duiden waarvan je de term x in rekening brengt voor de ontwikkeling. Bovendien is (per definitie) $\binom{n}{k} = 0$ als $k > n$. In woorden luidt deze formule: de voortbrengende functie voor de combinaties zonder herhaling van n elementen is $(1+x)^n$.

4. Hier zonder bewijs. Deze formule is echter van groot belang, omdat je hiermee een macht van de machtreeks $\sum_{k=0}^{\infty} x^k$ omzet in een machtreeks. In woorden: de voortbrengende functie voor de combinaties met herhaling van n elementen is $(1-x)^{-n}$.

De laatste twee formules tonen aan dat er een verband bestaat tussen voortbrengende functies en het uitvoeren van tellingen. □

De vier formules uit stelling 4.2 zetten een voortbrengende functie om in een som van 2 óf een som van oneindig veel termen. Omgekeerd, heb je één van deze sommen (of een som die daartoe te herleiden is), dan kan je deze som inkorten tot zijn voortbrengende functie. Bestaat er echter ook een omzettingsformule die je voorthelpt als je een som van m termen hebt $(m > 2)$?

Stelling 4.3.

voortbrengende functie	*tussen-vorm*	*formele machtreeks*
$\dfrac{1-x^m}{1-x}$	$= (1-x^m)(\sum_{k=0}^{\infty} x^k)$	$= \sum_{k=0}^{m-1} x^k$

Bewijs Straightforward rekenwerk, eens je de noemer van lid verwisseld hebt. Misschien is de formule herkenbaarder als je de volgorde van de termen omwisselt? Als je wat ervaring hebt met rekenwerk met veeltermen, zou je deze formule immers vlot moeten herkennen: $\dfrac{x^7-1}{x-1} = x^6+x^5+x^4+x^3+x^2+x+1$. □

Opmerking Bovenstaande formules zijn ook geldig als je x vervangt door een veelvoud of een macht van zichzelf. Vervangen we x bijvoorbeeld door $-x$, dan komt er

$$\frac{1}{1+x} = \sum_{k=0}^{\infty}(-x)^k = 1 - x + x^2 - x^3 + x^4 - ...$$

De voortbrengende functie van de rij $(1, -1, 1, -1, 1, -1, ...)$ is dus $\frac{1}{1+x}$. Onthoud alvast de variant voor de tweede formule: voor G een veelvoud of macht van x geldt er

$$\boxed{\frac{1}{1-G} = 1 + G + G^2 + G^3 + \dots}$$

Bovenstaande formules laten ons nu toe om te switchen van machtreeks naar voortbrengende functie en omgekeerd. Onderstaand voorbeeld zou je kunnen oplossen aan de hand van (saai) rekenwerk (ontwikkeling van $(1 + x + x^2 + x^3)^3$), maar als je de omkaderde omzettingen goed gebruikt kan je dit ook korter. (Aanrader: probeer de oefening met grotere getallen en merk het verschil tussen beide oplossingsmethodes!)

Voorbeeld

Zoek het aantal oplossingen in $\mathbb{N}[5, 8] = \{5, 6, 7, 8\}$ van de vergelijking $a + b + c = 17$. Hierbij is de oplossing $(a, b, c) = (6, 6, 5)$ niet gelijk aan de oplossing $(a, b, c) = (5, 6, 6)$. We zoeken dus 3 getallen uit $\{5, 6, 7, 8\}$ wier som gelijk is aan 17. Of:

$$\begin{aligned} a + b + c &= 17 \\ x^{a+b+c} &= x^{17} \\ x^a x^b x^c &= x^{17} \end{aligned}$$

Stellen we de verschillende keuzes voor a (nl. $5, 6, 7$ of 8) voor door de factor $(x^5 + x^6 + x^7 + x^8)$ (en analoog voor de verschillende keuzemogelijkheden voor b en c), dan zoeken we dus de coëfficiënt van x^{17} in de ontwikkeling van $(x^5 + x^6 + x^7 + x^8)^3$. Dit is gelijk aan de coëfficiënt van x^2 in $(1 + x + x^2 + x^3)^3$. Deze macht handmatig uitrekenen zou (nog net) gaan, maar toepassing van de omzettingen uit stellingen 4.2 en 4.3 gaat sneller - en deze methode is uitbreidbaar naar grotere getallen.

$$\begin{aligned} (1 + x + x^2 + x^3)^3 &= (1 - x^4)^3(1 + x + x^2 + x^3 + \dots)^3 \\ &= \textstyle\sum_{k=0}^{3} \binom{3}{k} (-x^4)^k \cdot \sum_{k=0}^{\infty} \binom{3+k-1}{k} x^k \\ &= [1 - \binom{3}{1} x^4 + \binom{3}{2} x^8 - x^{12}][1 + \binom{3}{1} x + \binom{4}{2} x^2 + \binom{5}{3} x^3 + \dots] \end{aligned}$$

De coëfficiënt van x^2 in deze ontwikkeling is $1 \cdot \binom{4}{2} = \frac{4!}{2!2!} = 6$.

Leid nu ook snel af hoeveel oplossingen er in $\mathbb{N}[5, 8]$ bestaan voor de vergelijkingen $a + b + c = 18$ en $a + b + c = 19$. Kan je een algemene formule ontdekken?
Antwoord voor 18 en 19: 10 en 12.

Oefening 1

Bepaal $g(x)$, zo dat $g(x)(1 + 2x + 3x^2 + 4x^3 + \dots) = 1$.

Oefening 2

Geef de genererende functie voor $(a_k)_{k\in\mathbb{N}}$, waarbij a_n gedefinieerd wordt door

1. *het aantal manieren om n drankjes te kiezen uit 3 flesjes fruitsap en 5 flesjes water.*
2. *het aantal manieren om n knikkers te kiezen uit een zak van 4 rode, 3 groene en 5 blauwe. De blauwe zitten echter samen verpakt: een zakje van 2 en een zakje van 3.*
3. *het aantal manieren om n gram schelpen te rapen van het strand, als een mosselschelp 2 gram weegt en een gewone schelp 3 gram. Controleer de kleine n-waarden met een uitgewerkte lijst!*
4. *het aantal manieren om n glazen te bestellen, als er 3 glazen melk zijn en zoveel glazen water als men wil.*
5. *het aantal manieren om n rode en gele knikkers te kiezen, als er minstens 4 rode en minstens 2 gele knikkers moeten zijn.*

Oefening 3

Zoek een uitdrukking voor a_k in termen van k, zodat je onderstaande genererende functies kan herschrijven als $\sum_{k=0}^{\infty} a_k x^k$.

1. $f(x) = (1 + x + x^2 + x^3 + \ldots)^2$
2. $f(x) = (1 + x + x^2 + x^3 + \ldots)(1 + x)$
3. $f(x) = (1 - x + x^2 - x^3 + \ldots)(1 + x)$

Oefening 4

Herneem de oefening op blz 62 met grotere getallen: geef het aantal oplossingen in $\mathbb{N}[5, 10] = \{5, 6, 7, 8, 9, 10\}$ van de vergelijking $a+b+c+d = 25$ respectievelijk $a+b+c+d = 26$. Hierbij is de oplossing $(5, 5, 5, 10)$ verschillend van de oplossing $(5, 5, 10, 5)$. (Hoeveel verschillende oplossingen zijn er, en kan je ze opsommen om je resultaat te controleren?)

4.5 Recurrente betrekkingen versus rechtstreekse formules

We haalden het al aan bij de definitie van de binomiaalcoëfficiënten: de grootheden $a_{n,k}$ uit het binomium van Newton, te weten $(x + y)^n = \sum_{k=0}^{\infty} a_{n,k} x^k y^{n-k}$, kan je ofwel opzoeken in de driehoek van Pascal (dit wil zeggen dat je om $a_{n,k}$ te kennen, je ook waarden $a_{i,j}$ moet berekenen met $i < n$ en $j < k$), ofwel maak je gebruik van de rechtstreekse formule $\binom{n}{k}$. Dat laatste is uiteraard heel wat sneller. De vraag is nu: kunnen we voor een recursief (of recurrent) gedefinieerde reeks $(a_k)_{k\in\mathbb{N}}$ een rechtstreekse formule vinden voor de algemene term a_k? Het antwoord is ja, zolang de recursieve definitie niet te ingewikkeld is. En bijvoorbeeld niet afhankelijk is van de index k, maar enkel van de voorgaande termen — en dit bovendien op een lineaire manier.

Bekijken we het probleem van de torens van Hanoï (zie blz 16). De recursieve (of recurrente) definitie van de $k$de term uit dit probleem werd gegeven door

$$\begin{aligned} m_1 &= 1 \\ m_k &= 2m_{k-1} + 1 \end{aligned}$$

Definiëren we $m_0 = 0$, dan geldt de recursieve definitie voor $k \geq 1$. De rij wordt dus $(m_0, m_1, m_2, \ldots)$. We stellen de voortbrengende functie van $(m_k)_{k \in \mathbb{N}}$ op:

$$\begin{array}{rrcl} & M & = & m_0 + m_1 x + m_2 x^2 + \ldots \\ & & = & m_0 + (2m_0 + 1)x + (2m_1 + 1)x^2 + \ldots \\ & & = & (2m_0 x + 2m_1 x^2 + \ldots) + x + x^2 + \ldots \\ & & = & 2Mx + x(1 + x + x^2 + \ldots) \\ \Leftrightarrow & M - 2Mx & = & x(1 + x + x^2 + \ldots) \\ \Leftrightarrow & M(1 - 2x) & = & x(1 + x + x^2 + \ldots) \\ & & = & x \, \frac{1}{1-x} \\ \Leftrightarrow & M & = & \dfrac{x}{(1-2x)(1-x)} \end{array}$$

Nu kennen we wel ontwikkelingen voor $\frac{1}{1-x}$ en $(\frac{1}{1-y})^n$, maar niet voor de gemengde vorm $(\frac{1}{1-x}) \cdot (\frac{1}{1-y})$ (met $y = 2x$ hier). Ontwikkelen we elke factor apart, dan zou ons dat een product van sommaties opleveren, wat uiteraard niet interessant is. Oplossing van dit probleem: we splitsen $\frac{x}{(1-2x)(1-x)}$ in partieelbreuken, dit wil zeggen we zoeken constanten a en b zodanig dat

$$\frac{x}{(1-2x)(1-x)} = \frac{a}{(1-2x)} + \frac{b}{(1-x)}.$$

We stellen

$$\begin{array}{rcl} \dfrac{x}{(1-2x)(1-x)} & = & \dfrac{a}{(1-2x)} + \dfrac{b}{(1-x)} = \dfrac{a(1-x) + b(1-2x)}{(1-2x)(1-x)} \\ & = & \dfrac{(a+b) + (-a-2b)x}{(1-2x)(1-x)}. \end{array}$$

Stellen we de coëfficiënten in de tellers gelijk, dan krijgen we $a + b = 0$ en $-a - 2b = 1$. Daaruit volgt dat $a = 1$ en $b = -1$. Waaruit

$$M = \frac{x}{(1-2x)(1-x)} = \frac{1}{1-2x} - \frac{1}{1-x}.$$

Uit de betrekking voor $\frac{1}{1-G}$ op blz 62 halen we nu snel een ontwikkeling voor beide termen:

$$\begin{array}{rcl} M & = & (1-2x)^{-1} - (1-x)^{-1} \\ & = & \sum_{k=0}^{\infty} (2x)^k - \sum_{k=0}^{\infty} x^k \\ & = & \sum_{k=0}^{\infty} 2^k x^k - \sum_{k=0}^{\infty} x^k \\ & = & \sum_{k=0}^{\infty} (2^k - 1) x^k \end{array}$$

Bij deze berekenden we dus een rechtstreekse formule voor het aantal zetten dat nodig is om de toren van Hanoï met n schijven te verzetten naar een andere stok.

Dezelfde methode kan gebruikt worden voor recurrente betrekkingen van hogere orde (dus als m_i afhankelijk is van meerdere directe voorlopers).

Oefening 5

Geef de directe formule voor de term s_n uit de rij $(s_n)_{n\in\mathbb{N}}$, die recursief gedefinieerd wordt door

$$s_0 = 0, \qquad s_1 = 1, \qquad s_n = 2s_{n-1} - s_{n-2}.$$

Oefening 6

Geef een directe formule voor de term s_n uit de rij $(s_n)_{n\in\mathbb{N}}$, die recursief gedefinieerd wordt door

$$s_0 = s_1 = 1, \qquad s_n = -s_{n-1} + 6s_{n-2}.$$

Oefening 7

BELANGRIJK *We maken codewoorden bestaande uit enkel cijfers ($0 \to 9$). Hoeveel codewoorden van lengte n bestaan er, als de som van het aantal drieën en zevens in een codewoord altijd oneven is?* **Deze oefening is niet makkelijk, maar eens je het systeem doorhebt ook niet moeilijk meer. Bekijk de hints in de aparte bijlage één voor één.**

Oefening 8

Zoek een uitdrukking voor de genererende functie $f(x)$ van de rij (s_n), als

$$s_0 = 2, \qquad s_1 = -1, \qquad s_2 = 1 \qquad en \qquad s_n = s_{n-1} - 3s_{n-2} + s_{n-3} \text{ voor } n \geq 3.$$

Oefening 9

Geef een formule voor een algemene term a_k van de rij $(a_k)_{k\in\mathbb{N}}$ als deze rij de volgende genererende functie $f(x)$ heeft:

1. $f(x) = \dfrac{1}{1-2x} + \dfrac{1}{1+x}$
2. $f(x) = \dfrac{2}{1-3x^2}$
3. $f(x) = \dfrac{-1}{1-2x} + \dfrac{4}{1+5x}$

Oefening 10

Toon de rechtstreekse formule voor een term uit de reeks van Fibonacci aan. Je vindt deze formule in de voetnoot op blz 15.

4.6 Homogene lineaire recurrente betrekkingen

Wie de laatste oefening heeft uitgewerkt, heeft gezien dat de omzetting van een recurrente betrekking voor een algemene reeksterm naar een rechtstreekse formule via de "straightforward"methode doenbaar is, maar bewerkelijk en dus foutgevoelig kan zijn (o.a. splitsen in partieelbreuken). Hier komt de theorie van de homogene lineaire betrekkingen ons ter hulp. We geven een kort overzicht van de juiste terminologie.[2]

Als een rij $(a_k)_{k\in\mathbb{N}}$ op een recursieve manier gedefinieerd wordt, dan krijgen we enerzijds een aantal specifieke startwaarden voor a_i $(i = 0, 1, \ldots, k-1)$, en anderzijds een vormingswet

$$a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k}), \qquad n \geq k.$$

Deze vormingswet wordt een **recurrente betrekking** voor de rij $(a_k)_{k\in\mathbb{N}}$ genoemd. Elke functie $g(n)$ zodanig dat $g(n) = a_n$ wordt een **oplossing van de betrekking** genoemd. Het is een rechtstreekse (niet-recursieve) formule voor a_n, zoals we in voorgaande oefeningen gezocht hebben. Tot nu toe gebruikten we in de uitwerking van een oplossing $g(n)$ de specifieke waarden van de termen $a_0, a_1, \ldots a_{k-1}$, die we de **vrijheidsgraden** van de recurrente betrekking noemen. Dit is echter niet noodzakelijk: we kunnen $a_0, a_1, \ldots a_{k-1}$ als symbool laten staan in de oplossing $g(n)$. Doen we dit, dan noemen we $g(n)$ de **algemene oplossing van de recurrente betrekking** $a_n = f(a_0, a_1, \ldots a_{n-k})$ $\quad n \geq k$. Geven we wél specifieke waarden aan alle $a_i (i : 0 \to k)$, dan spreken we van een **particuliere oplossing**.

Voorbeeld van een recurrente betrekking:

$$a_n = 7a_{n-1}^2 - n \cdot a_{n-2} \cdot a_{n-3} \qquad n \geq 3$$

Dit is duidelijk geen lineaire vergelijking in de parameter a_{n-j}. De/een oplossing $g(n)$ voor deze recurrente betrekking is niet makkelijk te vinden — er bestaat geen algemene methode voor. We beperken onze studie tot "bravere" recurrente betrekkingen.

Een recurrente betrekking van de vorm

$$s_n = c_1 s_{n-1} + c_2 s_{n-2} + c_3 s_{n-3} + \ldots + c_k s_{n-k}$$

met c_i (gekende) constanten en $c_k \neq 0$, is een **homogene lineaire recurrente betrekking van de orde k met constante coëfficiënten**.

homogeen:	omdat er geen constante term in de recurrente relatie voorkomt
lineair:	omdat de uitdrukking lineair is in elke s_{n-i}
orde k:	omdat s_n in functie van zijn k voorlopers gedefinieerd wordt (s_{n-1} tot s_{n-k})
constante coëff.:	omdat alle c_i constanten zijn, en bijvoorbeeld niet afhangen van n

Stelling 4.4. *Indien $g_i(n)$ $(i = 1, \ldots, m)$ oplossingen zijn van $s_n = c_1 s_{n-1} + \ldots + c_k s_{n-k}$ dan is elke lineaire combinatie $\sum_{i=1}^{m} \alpha_i g_i(n)$ $\quad (\alpha_i \in \mathbb{R})$ van deze m oplossingen, ook een oplossing van de betrekking.*

[2] Voor wie thuis studeert: informeer je eerst grondig over wat er in de les al dan niet gezien werd.

Bewijs Stel dat $h(n)$ een lineaire combinatie is van oplossingen $g_i(n)$, dus $h(n) = \sum_{i=1}^{m} \alpha_i g_i(n)$. Gezien $g_i(n)$ oplossing is van

$$s_n = c_1 s_{n-1} + c_2 s_{n-2} + \ldots + c_k s_{n-k} \qquad n \geq k$$

geldt

$$\begin{aligned} g_i(n) &= c_1 g_i(n-1) + c_2 g_i(n-2) + \ldots + c_k g_i(n-k) \\ &= \textstyle\sum_{l=1}^{k} c_l g_i(n-l) \end{aligned}$$

zodat

$$\begin{aligned} h(n) &= \textstyle\sum_{i=1}^{m} \alpha_i g_i(n) \\ &= \textstyle\sum_{i=1}^{m} \alpha_i \left(\sum_{l=1}^{k} c_l g_i(n-l) \right) \\ &= \textstyle\sum_{l=1}^{k} c_l \left(\sum_{i=1}^{m} \alpha_i g_i(n-l) \right) \\ &= \textstyle\sum_{l=1}^{k} c_l h(n-l) \end{aligned}$$

Bijgevolg is $h(n) = \sum_{i=1}^{m} \alpha_i g_i(n)$ oplossing van

$$s_n = c_1 s_{n-1} + c_2 s_{n-2} + \ldots + c_k s_{n-k}, \qquad n \geq k$$

□

Opmerking Een gelijkaardig resultaat geldt voor oplossingen van niet-homogene vergelijkingen, met een analoog bewijs. We hebben hier echter voldoende aan bovenstaande stelling.

4.7 Oplossen van homogene lineaire recurrente betrekkingen

Er bestaat een vrij eenvoudig algoritme om homogene lineaire recurrente betrekkingen op te lossen — efficiënter dan de lange uitwerking die voor bijvoorbeeld de laatste oefening op blz 65 nodig was.

Om de gedachte te vestigen concentreren we ons op homogene lineaire recurrente betrekkingen van de orde 2. Gegeven

$$s_n = a s_{n-1} + b s_{n-2},$$

zoek dan één/meerdere oplossingen $g_i(n)$ zodat

$$g_i(n) = a g_i(n-1) + b g_i(n-2).$$

We weten al dat — eens oplossingen g_i gevonden — elke lineaire combinatie $\sum_i \alpha_i g_i(n)$ een (algemene) oplossing zal zijn. De (nog onbepaalde) coëfficiënten α_i zullen ons toelaten om een particuliere oplossing te vinden, aangepast aan de specifieke waarden van de startelementen uit de reeks (dit wil zeggen s_0 en s_1, of s_1 en s_2). Nu bestaat de '*truuk*' van de oplossingstechniek erin om voor $g(n)$ een zodanige vorm te kiezen (nl. exponentiële), dat er inderdaad gepaste algemene oplossingen uit de bus komen.

Stelling 4.5. *Gegeven de recurrente betrekking*

$$s_n = a s_{n-1} + b s_{n-2},$$

dan is de functie $g(n) = r^n$ een oplossing van deze recurrente betrekking als en slechts als r oplossing is van de vergelijking

$$x^2 = ax + b.$$

Bewijs De functie $g(n) = r^n$ is een oplossing van de recurrente betrekking $s_n = as_{n-1} + bs_{n-2}$ als en slechts als

$$\begin{aligned} & g(n) = ag(n-1) + bg(n-2) \\ \Leftrightarrow \quad & r^n = ar^{n-1} + br^{n-2} \\ \Leftrightarrow \quad & r^2 = ar + b \end{aligned}$$

met andere woorden: als en slechts als r oplossing is van $x^2 = ax + b$. □

Een analoog resultaat geldt voor hogere orde recurrente betrekkingen. De vergelijking $x^2 = ax + b$ wordt de **karakteristieke vergelijking** van de recurrente betrekking genoemd.

Gevolg Zijn er twee verschillende wortels r_1, r_2 voor de karakteristieke vergelijking, dan is de algemene oplossing van de vorm $g(n) = \alpha_1 r_1^n + \alpha_2 r_2^n$ met α_1, α_2 willekeurig. Een particuliere oplossing behorend bij bepaalde waarden s_0, s_1 heeft dezelfde vorm, maar α_1 en α_2 zullen vastliggen door de waarden s_0 en s_1.

Is er één wortel r met multipliciteit 2 voor de karakteristieke vergelijking, dan bekom je uit de stelling enkel de partikuliere oplossing $g_1(n) = r^n = (\frac{a}{2})^n$ — te weinig om een algemene oplossing uit op te bouwen. We kunnen echter aantonen (bewijs als oefening) dat $g_2(n) = nr^n = n(\frac{a}{2})^n$ ook een oplossing is van $s_n = as_{n-1} + bs_{n-2}$. Zo komen we dus tot de algemene oplossing $g(n) = s_n = (\alpha_1 + n\alpha_2)r^n$ met α_1, α_2 willekeurig (of, voor een particuliere oplossing, α_1 en α_2 te bepalen uit s_0 en s_1).

Oefening 11

Gebruik de techniek van de karakteristieke vergelijking om een oplossing te vinden voor de recurrente betrekking van de Fibonaccireeks (zie blz 15 en blz 65).

Oefening 12

Zoek een oplossing voor de recurrente betrekking

1. $s_n = 6s_{n-1} - 9s_{n-2}$ *die voldoet aan* $s_0 = 1$ *en* $s_1 = 2$.
2. $s_n - 6s_{n-1} + 9s_{n-2} = 0$ *die voldoet aan* $s_0 = 5$ *en* $s_1 = 12$.
3. $2s_{n+2} - 11s_{n+1} + 5s_n = 0$ *die voldoet aan* $s_0 = 2$ *en* $s_1 = -8$.

Oefening 13

Vul de leemte in de redenering van het gevolg op blz 68 aan: bewijs dat $g_2(n) = nr^n = n(\frac{a}{2})^n$ *ook een particuliere oplossing is voor* $s_n = as_{n-1} + bs_{n-2}$, *als de bijhorende karakteristieke vergelijking maar één wortel heeft.*

Oefening 14

Kan je het besluit van de oplossingstechniek met de karakteristieke vergelijking voor homogene lineaire recurrente betrekkingen van orde 2 uitbreiden naar betrekkingen van orde k*? Een bewijs is niet nodig; herschrijf het besluit alleen.*

Oefening 15

Test je voorgaande antwoord op volgende recurrente betrekking:
$s_n - 3s_{n-1} - 6s_{n-2} + 28s_{n-3} - 24s_{n-4} = 0$, *met* $s_0 = 0$, $s_1 = 11$, $s_2 = -13$, $s_3 = -37$. *Uiteraard kan je zelf nagaan of je antwoord juist is: bereken met de gevonden* $g(x)$ *de eerste paar termen (ná* s_3*); en vergelijk dit met de uitkomst als je de recursieve definitie gebruikt.*

Hoofdstuk 5

Diophantische vergelijkingen: lineair

5.1 Rekenen in $\boldsymbol{Z}$

We haalden in de inleiding van de cursus aan, dat datgene wat wij de werkelijke wereld plachten te noemen, te weten de driedimensionale wereld[1] die door de fysische wetten van Newton, Einstein en mede-fysici beschreven wordt, nood heeft aan reële getallen. Vraagstukken omtrent deze leer, drukken zich bijgevolg uit in reële vergelijkingen waarvoor reële oplossingen gezocht worden.

De binnenkant van de computer echter, en dus ook deze cursus, werkt enkel met gehele getallen. Vraagstukken die hiermee verband houden, zullen dus uitgedrukt worden in vergelijkingen met gehele coëfficiënten (of desnoods breuken, maar geen niet-rationale grootheden), en vragen dan ook gehele oplossingen.

Elke vergelijking die uitgedrukt kan worden in gehele coëfficiënten en enkel gehele oplossingen vraagt, noemen we Diophantisch[2]. Elke Diophantische vergelijking heeft 0, een eindig aantal of een oneindig aantal oplossingen. In dat laatste geval kan je alle oplossingen aan de hand van één of meer gehele parameters opsommen.

Voorbeeld

> De oplossingen (x, y) van de Diophantische vergelijking $x^2 - 2y^2 = 0$ zal gegeven worden door de punten die op de (gedegenereerde) kromme $x^2 = 2y^2$ liggen, en gehele coördinaten hebben. Uiteraard geldt dit enkel voor het punt $(0, 0)$. De vergelijking $x^2 + y^2 = z^2$ daarentegen heeft een oneindig aantal oplossingen; deze stellen dan de punten (x, y, z) voor die op het driedimensionale oppervlak met

[1] In deze wereld werken we met de dimensies x, y en z. (De parameter t (voor tijd) wordt soms geïnterpreteerd als de vierde dimensie, hoewel er andere interpretatiemogelijkheden zijn.) De quantumfysica zit al heel wat dimensies verder, gesteund door moderne wiskunde.

[2] Naar Diophantus van Alexandrië (200-284 a.D.), auteur van 13 volumes 'Arithmetica'

vergelijking $x^2 + y^2 = z^2$ liggen, en gehele coördinaten hebben.

We houden ons in dit hoofdstuk enkel bezig met eenvoudige Diophantische vergelijkingen: de linaire gevallen. In hoofdstuk 6 volgt dan een bespreking van een aantal niet-lineaire vergelijkingen.

5.1.1 Bepaling van grootste gemene deler en oplossen van $\boxed{ax + by = c}$

Een begrip dat nauw verbonden is met de eenvoudige, lineaire Diophantische vergelijkingen is deelbaarheid. Immers, gezien we niet wensen te werken met reële getallen (en bij voorkeur ook niet met breuken), zullen we ons af en toe moeten afvragen of de bewerkingen die we wensen te doen wel resulteren in een natuurlijk getal. En dan stoten we vanzelf op de eerste bewerking die niet inwendig is in $\boldsymbol{Z}$: de deling. Daar kan het misgaan bij het oplossen van vergelijkingen. Vandaar de belangrijke plaats die deelbaarheid zal innemen in dit hoofdstuk.

Definitie. *Gegeven 2 gehele getallen a en b met $a \neq 0$. Als er een geheel getal c bestaat zodat $ac = b$, dan zeggen we a* **deelt** *b. In dat geval noteren we $a \mid b$, we noemen a een* **deler** *of* **factor** *van b, en b een* **veelvoud** *van a.*

Als a geen deler is van b, schrijven we $a \nmid b$. Als $a \mid b$ met a positief en verschillend van b, dan noemen we a een **eigenlijke deler van** *b. We zullen ons in wat volgt ook enkel bezighouden met eigenlijke delers. Is a bovendien groter dan 1, dan noemen we a een* **niet-triviale deler** *van b. De triviale delers van a zijn 1 en a zelf.*

De **grootste gemene deler van** *a* **en** *b is het grootste getal d waarvoor $d \mid a$ en $d \mid b$. Notatie: $ggd(a, b)$.*

Een **priemgetal** *p is een positief geheel getal dat enkel triviale delers heeft (nl. 1 en p). In de hoofdstukken over getaltheorie zal de letter p normaliter staan voor een priemgetal, de letter n voor een willekeurig (positief) geheel getal (al dan niet priem).*

Twee getallen a en b worden **relatief priem** *genoemd als $ggd(a, b) = 1$. Getallen $a_1, a_2, \ldots, a_k$ worden* **paarsgewijs relatief priem** *genoemd als $ggd(a_i, a_j) = 1$ voor $i \neq j$.*

Vóór we enkele eigenschappen van deelbaarheid opsommen en aantonen, komt eerst het delingsalgoritme aan bod. Dit drukt uit dat, ook als a geen deler is van b, we de deling op een unieke manier '*zo ver mogelijk*' kunnen uitvoeren – waarbij we dan met een rest (kleiner dan a) blijven zitten.

Stelling 5.1. Delingsalgoritme *Stel $a, b \in \mathbb{N}$, $a > 0$. Dan bestaan er unieke gehele getallen $q, r \in \mathbb{N}$ zodat*

$$b = aq + r \qquad 0 \leq r < a.$$

Hier is b het **deeltal**, *q het* **quotient**, *a de* **deler** *en r de* **rest**. *De rest r is strikt positief als en slechts als $a \nmid b$.*

Bewijs Beschouw de meetkundige reeks

$$\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots$$

dan is er een geheel getal q zo dat

$$qa \leq b < (q+1)a$$

Stel $b - qa = r$, dan is $b = aq + r$ met $0 \leq r < a$. Hiermee is het bestaan van q en r aangetoond. Nu nog de enigheid. Stel dat

$$\begin{array}{rll} & b = aq_1 + r_1 & 0 \leq r_1 < a \\ \text{en} & b = aq_2 + r_2 & 0 \leq r_2 < a \end{array}$$

We tonen aan dat $r_1 = r_2$. Stel dat $r_1 \neq r_2$, dus $r_1 < r_2$ (wissel indices indien nodig), dus

$$\begin{array}{rccccccc} & 0 & \leq & r_1 & < & r_2 & < & a \\ \overset{-r_1}{\Rightarrow} & & & 0 & < & r_2 - r_1 & < & a - r_1 \quad \leq \quad a \end{array}$$

Uit $b = aq_1 + r_1 = aq_2 + r_2$ volgt $0 = a(q_2 - q_1) + (r_2 - r_1)$, dus $a \mid (r_2 - r_1)$. In contradictie met $a > (r_2 - r_1)$. Daaruit volgt dat $r_1 = r_2$ en dus $q_1 = q_2$. □

Stelling 5.2. Priemontbinding *Elk geheel getal groter dan* 1 *kan op unieke manier geschreven worden als produkt van priemgetallen:*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

met $p_1, p_2, \ldots, p_k$ onderling verschillende priemgetallen, en $\alpha_1, \ldots, \alpha_k$ positieve gehele getallen. We noemen $\prod_{i=1}^{k} p_i^{\alpha_i}$ de **priemontbinding** *of* **priemfactorisatie** *van n.*

Bewijs Hier zonder bewijs (de enigheid van de ontbinding wordt bewezen aan de hand van een bewijs uit het ongerijmde, analoog aan stelling 5.1). □

Nu volgen enkele eigenschappen van deelbaarheid. De eerste spreken voor zich, de drie laatste verdienen wat meer aandacht (je hebt ze nog nodig, o.a. op blz 93).

Stelling 5.3. Eigenschappen van deelbaarheid *Stel $a, b, c, d, p, x, y \in \boldsymbol{Z}$; p priem.*
(a) $a \mid b$ en $a \mid c \Rightarrow a \mid (b + c)$
(b) $a \mid b \Rightarrow a \mid bc$
(c) $a \mid b$ en $b \mid c \Rightarrow a \mid c$
(d) $d = ggd(a, b) \Rightarrow d \mid ax + by$
(e) $a \mid bc \not\Rightarrow a \mid b$ of $a \mid c$
(f) $a \mid bc \Rightarrow \exists\, a_1, a_2$ zo dat $a_1 a_2 = a$, $a_1 \mid b$ en $a_2 \mid c$
(g) $p \mid bc \Rightarrow p \mid b$ of $p \mid c$

Bewijs
(a) Omdat a deler is van b, bestaat er een $k \in \boldsymbol{Z}$ zodat $ak = b$. Analoog bestaat er een l zodat $al = c$. Dus $ak + al = b + c$, of nog $a(k + l) = b + c$. Dus is a een deler van $b + c$.
(b) De uitspraak $a \mid b$ impliceert $ak = b$ voor zekere $k \in \boldsymbol{Z}$. Daaruit volgt $akc = bc$, voor

zekere $k \in \boldsymbol{Z}$. Stel $k' = kc$, dan zien we uit $ak' = bc$ dat a deler is van bc.
(c) Analoog te bewijzen.
(d) Analoog; als d grootste gemene deler is, deelt d zowel a als b.
(e) Tegenvoorbeeld: stel $a = 6$, $b = 4$, $c = 3$. We zien dat $6 \mid 12$, maar 6 deelt 4 noch 3.
(f) Stel $a \mid bc$, of nog: $ak = bc$ voor zekere $k \in \boldsymbol{Z}$. Beschouw de priemontbinding van deze 4 getallen:

$$\begin{aligned} a &= \textstyle\prod_{i=1}^{k} p_i^{\alpha_i} \\ b &= \textstyle\prod_{i=1}^{k} p_i^{\beta_i} \\ c &= \textstyle\prod_{i=1}^{k} p_i^{\gamma_i} \\ k &= \textstyle\prod_{i=1}^{k} p_i^{\kappa_i} \end{aligned}$$

Dan volgt hieruit dat $\alpha_i + \kappa_i = \beta_i + \gamma_i$, met $\alpha_i, \kappa_i, \beta_i, \gamma_i$ alle groter of gelijk aan nul. Daaruit volgt dat $\alpha_i = \beta_i + \gamma_i - \kappa_i$. Splits nu κ_i op in 2 (positieve) getallen κ_{1i}, κ_{2i} zodat $\beta_i - \kappa_{1i} \geq 0$ en $\gamma_i - \kappa_{2i} \geq 0$. Dit kan, vermits hun som $\alpha_i = (\beta_i - \kappa_{1i}) + (\gamma_i - \kappa_{2i})$ niet kleiner is dan 0. Stel nu

$$\begin{aligned} \alpha_{1i} &= \beta_i - \kappa_{1i} \\ \alpha_{2i} &= \gamma_i - \kappa_{2i}, \end{aligned}$$

dan is

$$a = \prod p_i^{\alpha_i} = \prod p_i^{\alpha_{1i}} p_i^{\alpha_{2i}} = \prod p_i^{\alpha_{1i}} \prod p_i^{\alpha_{2i}}.$$

Stellen we $a_1 = \prod p_i^{\alpha_{1i}}$ en $a_2 = \prod p_i^{\alpha_{2i}}$, dan zien we dat

$$a_1 = \prod p_i^{\alpha_{1i}} = \prod p_i^{(\beta_i - \kappa_{1i})} \mid \prod p_i^{\beta_i} = b$$

dus $a_1 \mid b$ en analoog $a_2 \mid c$, met $a_1 a_2 = a$.
(g) De enige mogelijke ontbindingen van p in 2 factoren zijn $p \cdot 1$ en $1 \cdot p$. Het eerste geval levert $p \mid b$ (en het triviale $1 \mid c$), het tweede geval levert $p \mid c$ (en $1 \mid b$). □

Volgende eigenschap is een sterkere versie van eigenschap (d). We tonen namelijk aan dat we x en y zó kunnen kiezen dat $d = ax + by$ in plaats van enkel $d \mid ax + by$ (met $d = \text{ggd}(a, b)$).

Stelling 5.4. Grootste gemene deler ggd(a, b) als lineaire combinatie van a en b
Stel a en b gehele getallen, niet beide nul. Dan bestaan er 2 gehele getallen x en y zodat

$$d = ggd(a, b) = ax + by.$$

Bewijs Beschouw de verzameling van alle lineaire combinaties $\{au + bv\}$, waar u en v alle waarden in $\boldsymbol{Z}$ overlopen. De verzameling $\{au + bv\}$ bevat zeker positieve en negatieve getallen, evenals nul.

We willen aantonen dat het kleinste (strikt positieve) veelvoud van d, d zelf, ook in de verzameling $\{au+bv\}$ zit. We nemen daartoe het kleinste strikt positieve getal uit de verzameling, noemen dit m, en tonen aan dat het voldoet aan de definitie van grootste gemene deler van a en b. Dan zal $m = d$.

1. Is het getal m deler van a? We delen a door m, en krijgen:

$$\begin{aligned} & a &=& \; mq + r && (0 \leq r < m) \\ \Rightarrow \; & r &=& \; a - mq \\ & &=& \; a - q(ax + by) \\ & &=& \; (1 - qx)a + (-qy)b \end{aligned}$$

Dus is r ook lineaire combinatie van a en b, dit wil zeggen $r \in \{au + bv\}$. Maar $r < m$, dus (uit definitie van m) volgt er $r = 0$. Daaruit volgt $a = mq$, of nog: $m \mid a$.

2. Is het getal m deler van b? Ja, analoge redering als voor $m \mid a$.

3. Is m de *grootste* gemene deler van a en b? Uit voorgaande blijkt dat m al zeker gemene deler is. Dit impliceert dat m kleiner is of gelijk aan de grootste gemene deler d ($m \leq d$). Maar m zit in $\{au + bv\}$, dus $d \mid m$ (eigenschap (d) uit stelling 5.3: d deelt elke lineaire combinatie van a en b). Dus $d \mid m$ én $m \leq d$. Daaruit volgt $m = d$.

□

Gevolg 5.5. *Twee getallen zijn relatief priem als en slechts als er getallen x en y bestaan zodat*

$$ax + by = 1.$$

Bewijs Stel a en b relatief priem, dus $\text{ggd}(a, b) = 1$. Dan garandeert stelling 5.4 dat er getallen x en y bestaan zodat $ax + by = 1$. Omgekeerd, stel dat $ax + by = 1$ en dat $d = \text{ggd}(a, b)$. Omdat $d \mid a$ en $d \mid b$, zal $d \mid ax + by$ of $d \mid 1$. Daaruit volgt $d = 1$. □

In woorden onthouden we:

Elke lineaire combinatie van a en b is een veelvoud van elk getal dat zowel a als b deelt. Er bestaat een lineaire combinatie die precies gelijk is aan de grootste gemene deler.

We weten nu dat de grootste gemene deler van a en b kan geschreven worden als lineaire combinatie van a en b, maar dit geeft ons nog geen snelle methode om de grootste gemene deler te bepalen. De missende schakel is het algoritme van Euclides. Dit algoritme geeft niet alleen een onfeilbare methode om $\text{ggd}(a, b)$ te vinden, maar het geeft ook (bij terugwerking van de stappen) de coëfficiënten x, y van de lineaire combinatie $ax + by = \text{ggd}(a, b)$.

Stelling 5.6. Algoritme van Euclides *Gegeven twee gehele getallen $a, b \in \mathbb{N}$, $a > b$. De grootste gemene deler van a en b wordt gegeven door volgende uitwerking.*

$$\begin{array}{rcll} a & = & bq_0 + r_1 & 0 < r_1 < b \\ b & = & r_1q_1 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2q_2 + r_3 & 0 < r_3 < r_2 \\ & \cdots & & \\ r_{n-2} & = & r_{n-1}q_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_nq_n + 0 & \end{array}$$

De laatste niet-triviale rest, nl. r_n, is de grootste gemene deler van a en b. Bovendien kunnen de waarden van x en y in $ggd(a, b) = ax + by$ bekomen worden door r_n (via r_{n-1}, r_{n-2},...) als lineaire combinatie van a en b te schrijven.

Bewijs **Deel 1** De methode baseert zich op volgende beschouwing. Als $d \mid a$ en $d \mid b$, dan $d \mid a + kb$ en $d \mid b$. We vervangen a dus door een lineaire combinatie van a en b. Het doel

is natuurlijk de berekeningen eenvoudiger te maken. Dus kiezen we de lineaire combinatie zodanig dat ze kleiner is dan a — zelfs kleiner dan b. En dan komt het delingsalgoritme van pas. Het getal a kan geschreven worden als $a = bq_0 + r_1$ met $0 \leq r_1 < b$, dus $a - bq_0 = r_1$ is lineaire combinatie van a en b die strikt kleiner is dan b. We hebben de kenmerkende eigenschap '$d \mid a$ en $d \mid b$' van een gemene deler dus omgezet naar '$d \mid b$ en $d \mid r_1$', met r_1 kleiner dan b. Het probleem is dus al verkleind, want b nam de plaats in van a ($b < a$), en r_1 nam de plaats in van b ($r_1 < b$). Herhalen we deze stap, dan volgt er '$d \mid r_1$ en $d \mid r_2$'. We zien dat het tweede deeltal (r_2 in het laatste geval) uiteindelijk vervangen wordt door nul. Want elke r_{i+1} is strikt kleiner dan r_i, maar niet-negatief. De laatste stappen zien er dan als volgt uit:

$$\begin{array}{lcll} r_{n-3} & = & r_{n-2}q_{n-2} + r_{n-1} & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} & = & r_{n-1}q_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_n q_n + 0 & \end{array}$$

De gevraagde grootste gemene deler is dan r_n, want $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n$.

Deel 2 We tonen nu nog aan dat de waarden van x en y in $\gcd(a,b) = ax + by$ kunnen bekomen worden door de stappen in het algoritme van Euclides achteruit te nemen. We zagen

$$\begin{array}{rcll} \gcd(a,b) & = & \gcd(b,r_1) & \text{met} \quad a - bq_0 = r_1 \\ & = & \gcd(r_1,r_2) & \text{met} \quad b - r_1q_1 = r_2 \\ & = & \gcd(r_2,r_3) & \text{met} \quad r_1 - r_2q_2 = r_3 \\ & \cdots & & \\ & = & \gcd(r_{n-2},r_{n-1}) & \text{met} \quad r_{n-3} - r_{n-2}q_{n-2} = r_{n-1} \quad (\bullet) \\ & = & \gcd(r_{n-1},r_n) & \text{met} \quad r_{n-2} - r_{n-1}q_{n-1} = r_n \quad (\star) \\ & = & \gcd(r_n,0) & \text{met} \quad r_{n-1} - r_nq_n = 0 \end{array}$$

We zien uit $(\star)$ dat $\gcd(a,b) = r_n$ uit te drukken is als lineaire combinatie van r_{n-1} en r_{n-2}. Vervangen we r_{n-1} vervolgens door de uitdrukking gegeven in $(\bullet)$, dan krijgen we:

$$\begin{array}{rcl} r_n & \overset{(\star)}{=} & r_{n-2} - r_{n-1}q_{n-1} \\ & \overset{(\bullet)}{=} & r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1} \\ & = & -q_{n-1}r_{n-3} + (1 + q_{n-2}q_{n-1})r_{n-2} \end{array}$$

We hebben een lineaire combinatie in r_{n-2} en r_{n-1} dus omgezet naar een lineaire combinatie in r_{n-3} en r_{n-2}. Zo verdergaand, zien we dat de grootste gemene deler kan geschreven worden als lineaire combinatie van a en b. We hadden stelling 5.4 dus ook via deze constructie kunnen bewijzen — dankzij het algoritme van Euclides.

Voorbeeld

Schrijf $\gcd(336, 1768)$ als $336 \cdot x + 1768 \cdot y$.
Uiteraard moeten we eerst de grootste gemene deler vinden.

$$\begin{array}{rcl} 1768 & = & 5 \cdot 336 + 88 \\ 336 & = & 3 \cdot 88 + 72 \\ 88 & = & 1 \cdot 72 + 16 \\ 72 & = & 4 \cdot 16 + 8 \\ 16 & = & 2 \cdot 8 + 0 \end{array}$$

De grootste gemene deler is dus 8. Daarna doorlopen we de stappen in omgekeerde volgorde, waarbij we de vermenigvuldigingen uiteraard niet expliciet uitwerken. (Let op: we starten bij de voorlaatste regel van voorgaande afleiding!)

$$\begin{aligned} 8 &= 72 - 4 \cdot 16 \\ &= 72 - 4(88 - 1 \cdot 72) \\ &= -4 \cdot 88 + 5(336 - 3 \cdot 88) \\ &= 5 \cdot 336 - 19 \cdot 88 \\ &= 5 \cdot 336 - 19(1768 - 5 \cdot 336) \\ &= -19 \cdot 1768 + 100 \cdot 336 \end{aligned}$$

... en natuurlijk niet vergeten narekenen!

Het algoritme van Euclides laat ons toe de lineaire combinatie van a en b te vinden, die precies gelijk is aan hun grootste gemene deler. Dit levert meteen een oplossingsmethode voor de lineaire Diophantische vergelijkingen in twee onbekenden.

Stelling 5.7. *Gegeven $a, b, c \in \boldsymbol{Z}$, met a en b niet beide nul. De lineaire Diophantische vergelijking*

$$ax + by = c$$

heeft oplossingen in x en y als en slechts als c veelvoud is van $ggd(a, b)$. Als (x_0, y_0) een oplossing is, dan is de algemene oplossing van de vorm

$$(x, y) = \left(x_0 + \frac{b}{d}\, t \;\;,\;\; y_0 - \frac{a}{d}\, t\right) \qquad\qquad t \in \boldsymbol{Z},\ d = ggd(a, b).$$

Bewijs **Deel 1** We bewijzen dat de voorwaarde 'c is veelvoud van $\text{ggd}(a, b)$' zowel nodig als voldoende is (zie blz 43 voor de juiste interpretatie van deze begrippen), om gehele oplossingen voor x en y te vinden. Stel $d = \text{ggd}(a, b)$, voor eenvoud van notatie. $\boxed{\Leftarrow}$ De voorwaarde is voldoende: áls c veelvoud is van d, dan is $c = k \cdot d$. We kunnen uit stelling 5.4 (of de formulering op blz 74) d schrijven als $ax_0 + by_0$ voor zekere x_0, y_0. Dus is c gelijk aan $k \cdot (ax_0 + by_0) = a(kx_0) + b(ky_0)$. Met andere woorden $(x, y) = (kx_0, ky_0)$ is oplossing van $ax + by = c$. $\boxed{\Rightarrow}$ De voorwaarde is nodig: stel dat (x_0, y_0) een oplossing is van de Diophantische vergelijking. Dan geldt er $ax_0 + by_0 = c$. Gezien $d \mid a$ en $d \mid b$, zal $d \mid c$.
Deel 2 Het is een triviale rekenoefening om na te gaan dat $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ een oplossing is als (x_0, y_0) een oplossing is. We moeten wel nog aantonen dat we geen enkele oplossing vergeten zijn. Stel (x_0, y_0) is een oplossing. Dan zoeken we, gerangschikt volgens x-waarde, het eerstvolgende koppel gehele getallen (x', y') dat ook oplossing is. We zoeken dus e, f met $e \in \mathbb{N}_0$ zo klein mogelijk en $f \in \boldsymbol{Z}$, zodat $(x_0 + e, y_0 + f)$ ook oplossing is.

$$\begin{aligned} & (x_0 + e, y_0 + f) \text{ is oplossing als } (x_0, y_0) \text{ oplossing is} \\ \Leftrightarrow\ & a(x_0 + e) + b(y_0 + f) = c \text{ met } ax_0 + by_0 = c \\ \Leftrightarrow\ & ae + bf = 0 \\ \Leftrightarrow\ & f = -\frac{a}{b}e \end{aligned}$$

Het gezochte geheel getal f kan dus uitgedrukt worden in functie van e. Maar f moet geheel zijn, dit impliceert $b \mid ae$. Stellen we $d = \text{ggd}(a, b)$ dan kunnen we $a = a'd$ en $b = b'd$ schrijven,

waarbij a' en b' onderling ondeelbaar zijn.

$$\begin{array}{|ll|l} & b \mid ae & \\ \Leftrightarrow & b'd \mid a'de & \\ \Leftrightarrow & b' \mid a'e & \\ \Rightarrow & b' \mid e & a', b' \text{ onderling ondeelbaar} \\ \Leftrightarrow & e \text{ is veelvoud van } b' & \\ \Leftrightarrow & e \text{ is veelvoud van } \dfrac{b}{d} & \end{array}$$

Omdat we $e \in \mathbb{N}_0$ zo klein mogelijk willen hebben, besluiten we $e = \frac{b}{d}$. Daaruit volgt $f = -\frac{a}{b}\frac{b}{d} = -\frac{a}{d}$. We vonden dus de eerstvolgende oplossing ná (x_0, y_0) (gerangschikt volgens stijgende x-waarden als $b > 0$, gerangschikt volgens dalende x-waarden als $b < 0$):

$$\left(x_0 + \frac{b}{d}, y_0 - \frac{a}{d}\right).$$

Met inductie volgt dan dat álle oplossingen gegeven worden door

$$\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right), \qquad t \in \boldsymbol{Z}.$$

□

Voorbeeld

Bepaal de oplossing(en) $(x, y) \in \boldsymbol{Z} \times \boldsymbol{Z}$ van de vergelijking $1734x + 221y = 340$.

We weten dat elke lineaire combinatie van 1734 en 221 een veelvoud is van de grootste gemene deler van 1734 en 221. Daarom bepalen we eerst deze grootste gemene deler (met het algoritme van Euclides). Na enig rekenwerk vinden we de grootste gemene deler (nl. 17), en de lineaire combinatie die gelijk is aan de grootste gemene deler:

$$1734(6) + 221(-47) = 17$$

Omdat het rechterlid van de opgave niet 17 is maar 340, moeten we uiteraard nog beide leden vermenigvuldigen in de gelijkheid hier net boven.

$$1734(6 \cdot 20) + 221(-47 \cdot 20) = 17 \cdot 20$$

Daaruit halen we al één oplossing van de gegeven vergelijking: $(x_0, y_0) = (120, -940)$. De algemene oplossing wordt gegeven door

$$(x, y) = (120 + 13t, -940 - 102t), \qquad t \in \boldsymbol{Z}$$

5.2 Rekenen in $\mathbb{Z}/_{n\mathbb{Z}}$

In de vorige paragraaf leerden we rekenen in $\mathbb{Z}$. Dit ligt al dichter bij de bitbewerkingen die een computer uitvoert, dan rekenen in $\mathbb{R}$. Toch zijn we er nog niet helemaal. Stelt men met een 32-bitspatroon natuurlijke getallen voor, dan weet je dat ná het getal 0 (bitpatroon 00..00) het getal 1 volgt (bitpatroon 00..01). Ná het getal $2^{32}-1$ (bitpatroon 11..11) volgt echter 0 in plaats van 2^{32}. En $(2^{32}-1)+x$ is gelijk aan $x-1$ (als $x < 2^{32}$). Met andere woorden: de computer rekent in dit geval automatisch modulo 2^{32}. Vandaar dat modulair rekenen hier het logische verlengstuk vormt op vorige paragraaf.

Definitie. *Stel $a, n \in \mathbb{Z}$ en $n > 1$.*

$r = a \bmod n$	*wordt gelezen als 'r is a modulo n' of*
	'r is de rest van a bij deling door n'
	(gevolg: $a \leq r < n$ en $r = a - \lfloor \frac{a}{n} \rfloor n$)
$a \equiv b \bmod n$	*wordt gelezen als 'a is congruent met b modulo n'*
	en staat voor $a \bmod n = b \bmod n$
	(let op: hier hoeven a noch b kleiner te zijn dan n.
	zodra je een gewoon gelijkheidsteken schrijft,
	onderstel je wél dat het linkerlid kleiner is dan n)

Er zijn heel wat equivalente notaties voor de uitspraak $a \equiv b \bmod n$. Belangrijk hierbij is:

- maak correct gebruik van '$=$' dan wel '$\equiv$'.
- zet om naar notaties die noch '$\equiv$' noch ' mod ' bevatten als je aan bepaalde rekenregels voor modulair rekenen twijfelt.

Alternatieve notaties voor $a \equiv b$ mod n

$$
\begin{aligned}
& a \equiv b \bmod n \\
\Leftrightarrow\ & a \bmod n = b \bmod n \\
\Leftrightarrow\ & a - kn = b - ln \qquad \text{voor zekere } k, l \in \mathbb{Z} \\
\Leftrightarrow\ & a + kn = b + ln \qquad \text{voor zekere } k, l \in \mathbb{Z} \\
\Leftrightarrow\ & a = b + kn \qquad \text{voor zekere } k \in \mathbb{Z} \\
\Leftrightarrow\ & a - b = kn \qquad \text{voor zekere } k \in \mathbb{Z} \\
\Leftrightarrow\ & n \mid (a - b)
\end{aligned}
$$

Twee getallen zijn dus congruent modulo n als ze dezelfde rest bij deling door n hebben. De congruentierelatie ($\equiv$) is reflexief, symmetrisch en transitief, net zoals de '*ordinaire*' gelijkheid:

Stelling 5.8. *Stel n een positief geheel getal. De congruentierelatie modulo n is een equivalentierelatie op de verzameling $\mathbb{Z}$, nl.*

reflexief	$a \equiv a \pmod n$	$\forall a \in \mathbb{Z}$
symmetrisch	$a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$	$\forall a, b \in \mathbb{Z}$
transitief	$a \equiv b \pmod n$ en $b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$	$\forall a, b, c \in \mathbb{Z}$

Bewijs Als oefening. Elimineer $\equiv$ en mod uit de notaties: vervang de uitspraak '$a \equiv \mod n$' door de uitspraak '$a = b + kn$ (voor zekere $k \in \boldsymbol{Z}$)'. □

Vorige stelling zegt dat de congruentierelatie een equivalentierelatie is op $\boldsymbol{Z}$. Hoewel de congruentierelatie '$\equiv$' volledig wordt opgebouwd aan de hand van de deelbaarheidsrelatie ' | ' (en in die zin dus niets nieuws is), zien we hier toch het voordeel van '$\equiv$' ten opzichte van ' | ': de deelbaarheidsrelatie is níet symmetrisch ($a \mid b \not\Rightarrow b \mid a$), en is dus geen equivalentierelatie. De congruentierelatie modulo n deelt $\boldsymbol{Z}$ op in n verschillende equivalentieklassen. In getaltheorie spreken we van de **congruentieklassen**, **residuklassen** of **restklassen**. Formeel:

$$\begin{aligned} [a]_n &= \{x \mid x \in \boldsymbol{Z} \text{ en } x \equiv a \pmod{n}\} \\ &= \{a + kn \mid k \in \boldsymbol{Z}\} \end{aligned}$$

Gezien $[a]_n = [a + ln]_n = [a - ln]_n = \ldots$, doen we er goed aan de notatie voor een equivalentieklasse éénduidig te maken door een vaste representant van de klasse te kiezen. Dit wordt het kleinste niet-negatieve getal a uit de congruentieklasse. Dit getal a is dus kleiner dan n (anders is $a - n$ kleiner dan a en toch nog niet negatief). Merk op: het is uiteraard niet uitgesloten om een klasse met een andere representant aan te duiden, maar in theoretische beschouwingen maken we graag die vooronderstelling. De verzameling van alle residuklassen modulo n wordt genoteerd als

$$\boldsymbol{Z}/_{n\boldsymbol{Z}} = \{[a]_n \mid 0 \leq a < n\}.$$

Merk op: in hoofdstuk 1 zagen we de definitie

$$\boldsymbol{Z}/_{n\boldsymbol{Z}} = \{0, 1, 2, \ldots, n-1\}.$$

Dit is uiteraard equivalent met bovenstaande definitie, in zoverre we 0 interpreteren als de restklasse $[0]_n$, 1 als de restklasse $[1]_n$ enzovoort. In plaats van de congruentieklasse, wordt enkel zijn representant gebruikt — maar de onderliggende klasse hou je best in gedachten! (Zo is -2 in $\boldsymbol{Z}/_{5\boldsymbol{Z}}$ gelijk aan 3.)

5.2.1 Rekenregels in $\boldsymbol{Z}/_{n\boldsymbol{Z}}$

Om vlot te rekenen in $\boldsymbol{Z}/_{n\boldsymbol{Z}}$, kunnen we rekenregels opstellen zoals in $\boldsymbol{Z}$. We weten dat de verzameling $\boldsymbol{Z}$ met de binaire operatoren $+$ en $\cdot$ een commutatieve ring met eenheidselement vormt. We kunnen nl. alle eigenschappen uit bijlage D één voor één controleren; dit vormen de rekenregels waaraan we ons in $\boldsymbol{Z}$ moeten houden (of beter: die logischerwijze volgen uit de fysische betekenis van optellen en vermenigvuldigen van gehele grootheden). Voor $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ kunnen we hetzelfde doen: we definiëren een bewerking $+$ en een bewerking $\cdot$, en controleren dan of de eigenschappen van deze bewerkingen ook voldoen aan de voorwaarden voor een commutatieve ring met eenheidselement. Gezien we de bewerkingen in $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ kunnen terugvoeren op bewerkingen in $\boldsymbol{Z}$, zal dit eenvoudig aan te tonen zijn. We hebben echter méér: we kunnen aantonen dat – voor bepaalde n – de verzameling $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ met bewerkingen $+, \cdot$ een veld is. Dit vereist de bijkomende eigenschap dat elk element (uitgezonderd 0) een invers heeft voor de vermenigvuldiging.

Eerst tonen we aan dat de congruentieklassen stabiel zijn onder de optelling, vermenigvuldiging en machtsverheffing in $\boldsymbol{Z}/_{n\boldsymbol{Z}}$: de congruentieklasse die hoort bij de som van twee representanten zal goed gedefinieerd zijn, ongeacht de keuze van de representant. Analoog voor de andere bewerkingen.

Stelling 5.9. *Gegeven $a, b, A, B \in \boldsymbol{Z}$. Als $[a]_n = [A]_n$ en $[b]_n = [B]_n$, dan geldt*

$$\begin{aligned} [a \pm b]_n &= [A \pm B]_n \\ [a \cdot b]_n &= [A \cdot B]_n \\ [a^m]_n &= [A^m]_n \end{aligned}$$

Bewijs We schrijven $a = A+kn$ en $b = B+ln$, daaruit volgt $[a+b]_n = [A+kn+B+ln]_n = [A+B]_n$. Deel 2 analoog, deel 3 met inductie. □

Dit laat ons nu toe volgende bewerkingen op congruentieklassen te definiëren:

$$\begin{aligned} [a]_n + [b]_n &= [a+b]_n \\ [a]_n - [b]_n &= [a-b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n \\ [a]_n^m &= [a^m]_n \end{aligned}$$

Uit bovenstaande definities én de stabiliteit volgen dan onmiddellijk de eigenschappen van optelling en vermenigvuldiging in $\boldsymbol{Z}/_{n\boldsymbol{Z}}$.

Stelling 5.10. *De verzameling $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ met bewerkingen $\{+, \cdot\}$ is een commutatieve ring met eenheidselement.*

Bewijs We kunnen aantonen dat volgende gelijkheden opgaan (zie bijlage D):

(1)	$[x] + [y] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$	$\forall [x], [y] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(2)	$([x] + [y]) + [z] = [x] + ([y] + [z])$	$\forall [x], [y], [z] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(3)	$[x] + [y] = [y] + [x]$	$\forall [x], [y] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(4)	$[0] + [x] = [x] = [x] + [0]$	$\forall [x] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(5)	$[x] + [-x] = [0]$	$\forall [x] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(1′)	$[x] \cdot [y] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$	$\forall [x], [y] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(2′)	$([x] \cdot [y]) \cdot [z] = [x] \cdot ([y] \cdot [z])$	$\forall [x], [y], [z] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(3′)	$[x] \cdot [y] = [y] \cdot [x]$	$\forall [x], [y] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(4′)	$[1] \cdot [x] = [x] = [x] \cdot [1]$	$\forall [x] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$
(6′)	$[x] \cdot ([y] + [z]) = ([x] \cdot [y]) + ([x] \cdot [z])$	$\forall [x], [y], [z] \in \boldsymbol{Z}/_{n\boldsymbol{Z}}$

Dit doen we door de beweringen in $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ terug te voeren op uitspraken in $\boldsymbol{Z}$. (Dit zal ook tijdens de oefeningen zijn nut bewijzen!) □

5.2.2 Oplossen van $\boxed{x \equiv \frac{1}{a} \bmod n}$

Nu dient zich echter de deling aan: in $\boldsymbol{Z}$ is ze niet (altijd) mogelijk — we moeten $\boldsymbol{Z}$ uitbreiden tot $\boldsymbol{Q}$ om de verzameling wél gesloten te maken voor de deling. Maar hoe zit het met $\boldsymbol{Z}/_{n\boldsymbol{Z}}$?

Voorbeeld

$\frac{4}{5} \equiv 8 \pmod{12}$ want $4 \equiv (5 \cdot 8) \pmod{12}$
$\frac{5}{4} \equiv \perp \pmod{12}$ (is onmogelijk) want er is geen enkel getal $x \in \{0, 1, \ldots, 11\}$ waarvoor $5 \equiv 4 \cdot x \pmod{12}$. (Ga na of bewijs korter.)

Natuurlijk is het te bewerkelijk (zeker voor grote n) om een bewering zoals die laatste steeds volledig na te trekken. Dit komt trouwens (qua werk) overeen met het opstellen van een vermenigvuldigingstabel: veel te veel voorbereiding én opzoekingswerk, zeker voor grote n.

We moeten dus een andere manier zoeken om te bepalen wanneer een deling $\frac{a}{b} \pmod n$ mogelijk is. Merk eerst op dat $\frac{a}{b} \equiv a \cdot \frac{1}{b} \pmod n$, zodat $\frac{a}{b} \pmod n$ met $\text{ggd}(a, b) = 1$ mogelijk is als en slechts als $\frac{1}{b} \pmod n$ mogelijk is. We noemen $\frac{1}{b} \pmod n$ het **multiplicatief invers** of **modulair inverse** van b modulo n. Of nog: twee getallen x en y zijn elkaars inverse voor de vermenigvuldiging als

$$xy \equiv 1 \pmod n$$

met $n > 1$.

Het is nu duidelijk dat, voor gegeven (x, n), het getal y niet altijd bestaat. Kijk maar op blz 9: niet elke kolom in de vermenigvuldigingstabel voor $\boldsymbol{Z}/_{8\boldsymbol{Z}}$ bevat een 1, dus de getallen 2, 4 en 6 hebben geen modulair invers in $\boldsymbol{Z}/_{8\boldsymbol{Z}}$. (Het getal 0 heeft uiteraard nooit een modulair invers.)

Stelling 5.11. *Het modulair inverse element y van x in $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ vinden, komt overeen met het oplossen van een Diophantische vergelijking:*

$$xy \equiv 1 \text{ (mod } n\text{) heeft een oplossing in } \boldsymbol{Z}/_{n\boldsymbol{Z}}$$
$$\Leftrightarrow \qquad \exists k \in \boldsymbol{Z} : xy + kn = 1$$

Hierbij zijn x en n gegeven, en k en y gezocht. Dit leidt ons tot volgende stellingen.

Stelling 5.12. *Het multiplicatief inverse $\frac{1}{b}$ (mod n) bestaat als en slechts als ggd$(b, n) = 1$.*

Stelling 5.13. *De deling $\frac{a}{b}$ (mod n) (waarbij ggd$(a, b) = 1$) is mogelijk als en slechts als ggd$(b, n) = 1$.*

Ga na met het voorbeeld van $\boldsymbol{Z}/_{8\boldsymbol{Z}}$.

Kunnen we ook voorspellen hoeveel getallen $x \in \{1, 2, \ldots, n-1\}$ er wél een multiplicatief invers zullen hebben, en welke geen? Dan moeten we dus het aantal getallen $< n$ kennen dat onderling ondeelbaar is met n. Dit getal is $\phi(n)$: de functiewaarde van de Euler-ϕ-functie voor n (zie bijlagen).

Stelling 5.14. *$\boldsymbol{Z}/_{n\boldsymbol{Z}}$ is een veld als en slechts als n priem is.*

Bewijs We weten al dat $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ (met n willekeurig) een commutatieve ring met eenheidselement is. Rest er aan te tonen dat elke element een invers element heeft voor de vermenigvuldiging. Uit stelling 5.12 volgt dat dit enkel het geval is als $\text{ggd}(b, n) = 1$ $\forall b \in \{0, 1, 2, \ldots, n-1\}$. Dus als en slechts als n priem is. □

Voorbeeld

Gebruik stelling 5.11 om de deling $\frac{1}{945}$ mod 1188 uit te werken.

$$\begin{array}{rrcll} & y & \equiv & \dfrac{1}{945} \bmod 1188 & \\ \Leftrightarrow & 945y & \equiv & 1 \bmod 1188 & \\ \Leftrightarrow & 945\, y + k\, 1188 & = & 1 & \text{voor zekere } k \in \boldsymbol{Z} \end{array}$$

We berekenen $\text{ggd}(945, 1188)$.

$$\begin{array}{rcl} 1188 & = & 1 \cdot 945 + 243 \\ 945 & = & 3 \cdot 243 + 216 \\ 243 & = & 1 \cdot 216 + 27 \\ 216 & = & 8 \cdot 27 + 0 \\ \Rightarrow & & \text{ggd}(945, 1188) = 27 \end{array}$$

Dus is de deling $\frac{1}{945}$ onmogelijk in $\boldsymbol{Z}/_{1188\boldsymbol{Z}}$.

Voorbeeld

Gebruik stelling 5.11 om de deling $\frac{1}{945}$ mod 2288 uit te werken.

$$\begin{array}{rrcll} & y & \equiv & \dfrac{1}{945} \bmod 2288 & \\ \Leftrightarrow & 945y & \equiv & 1 \bmod 2288 & \\ \Leftrightarrow & 945y + k2288 & = & 1 & \text{voor zekere } k \in \boldsymbol{Z} \end{array}$$

We berekenen $\text{ggd}(945, 2288)$.

$$\begin{array}{rcl} 2288 & = & 2 \cdot 945 + 398 \\ 945 & = & 2 \cdot 398 + 149 \\ 398 & = & 2 \cdot 149 + 100 \\ 149 & = & 1 \cdot 100 + 49 \\ 100 & = & 2 \cdot 49 + 2 \\ 49 & = & 24 \cdot 2 + 1 \\ 2 & = & 2 \cdot 1 + 0 \\ \Rightarrow & & \text{ggd}(945, 2288) = 1 \end{array}$$

Dus is de deling $\frac{1}{945}$ wel mogelijk in $\boldsymbol{Z}/_{2288\boldsymbol{Z}}$. We werken in omgekeerde volgorde:

$$\begin{aligned}
1 &= 49 - 24 \cdot 2 \\
&= 49 - 24(100 - 2 \cdot 49) \\
&= -24 \cdot 100 + 49 \cdot 49 \\
&= -24 \cdot 100 + 49(149 - 1 \cdot 100) \\
&= 49 \cdot 149 - 73 \cdot 100 \\
&= 49 \cdot 149 - 73(398 - 2 \cdot 149) \\
&= -73 \cdot 398 + 195 \cdot 149 \\
&= -73 \cdot 398 + 195(945 - 2 \cdot 398) \\
&= 195 \cdot 945 - 463 \cdot 398 \\
&= 195 \cdot 945 - 463(2288 - 2 \cdot 945) \\
&= -463 \cdot 2288 + 1121 \cdot 945
\end{aligned}$$

Dus $\frac{1}{945} \bmod 2288 \equiv 1121$. (Reken je antwoord altijd na!)

Voorbeeld

Bereken $\frac{22}{945} \bmod 2288$.

Antwoord: $\frac{22}{945} \bmod 2288 = (22 \cdot \frac{1}{945}) \bmod 2288 = 22 \cdot (\frac{1}{945} \bmod 2288) = 22 \cdot 1121 \bmod 2288 = 24662 \bmod 2288 = 1782$. Reken na!

5.3 Lineaire congruenties en oplossen van $\boxed{ax \equiv b \bmod n}$

We zagen rekenregels voor optelling en vermenigvuldiging in $\mathbf{Z}/_{n\mathbf{Z}}$, én een methode om de deling uit te voeren — indien gedefinieerd. We hebben dus genoeg bagage om lineaire vergelijkingen in $\mathbf{Z}/_{n\mathbf{Z}}$ op te lossen. Elke lineaire vergelijking in één onbekende in $\mathbf{Z}/_{n\mathbf{Z}}$, of **lineaire congruentie** van de vorm $ax \equiv b \pmod{n}$ is equivalent met een lineaire Diophantische vergelijking $ax + ny = b$. We zullen in de oefeningen dus terugwerken naar deze Diophantische vergelijking om de oplossing(en) te zoeken met Euclides; bij het formuleren van het antwoord zullen we echter nauwkeurig moeten zijn: worden er oplossingen verwacht in $\mathbf{Z}$ of in $\mathbf{Z}/_{n\mathbf{Z}}$? Afhankelijk daarvan zullen er oneindig veel of eindig veel oplossingen zijn (áls er zijn).

Stelling 5.15. *Stel ggd$(a, n) = d$. De lineaire congruentie $ax \equiv b$ (mod n) heeft oplossingen als en slechts als $d \mid b$. Er zijn dan d oplossingen gegeven door*

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

met x_0 de unieke oplossing van de lineaire congruentie

$$\frac{a}{d}x \equiv \frac{b}{d} \ (mod\ \frac{n}{d}).$$

Bewijs De lineaire congruentie $ax \equiv b \pmod{n}$ heeft oplossingen als en slechts als er een k en x in $\mathbf{Z}$ bestaan waarvoor $ax + kn = b$. Uit stelling 5.7 op blz 76 volgt dat dit het geval is als en slechts als b veelvoud is van ggd(a, n).
Stel x_0 een dergelijke oplossing, dan weten we uit diezelfde stelling dat elke bijkomende oplossing van de vorm $x_0 + t\frac{n}{d}$ is ($t \in \mathbf{Z}$). We hebben dus oplossingen van de vorm

$$\ldots, x_0 - 2\frac{n}{d}, x_0 - 1\frac{n}{d}, x_0, x_0 + 1\frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots$$

Maar omdat $x_0 + d\frac{n}{d} = x_0 + n \equiv x_0 \pmod{n}$, zijn er slechts d verschillende oplossingen in $\mathbf{Z}/_{n\mathbf{Z}}$. □

Voorbeeld

Los op in $\mathbf{Z}/_{270\mathbf{Z}}$: $48 \cdot x = 54$.
Anders gezegd: los de lineaire congruentie $48x = 54 \pmod{270}$ op. We gaan eerst na of dit wel oplosbaar is: we berekenen ggd$(48, 270)$.

$$\begin{aligned} 270 &= 5 \cdot 48 + 30 \\ 48 &= 1 \cdot 30 + 18 \\ 30 &= 1 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Dus ggd$(48, 270) = 6$, en dit deelt 54. Er zijn bijgevolg 6 oplossingen. Voor één van de oplossingen verwerken we het algoritme van Euclides in omgekeerde

volgorde.

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ &= 18 - 1(30 - 1 \cdot 18) \\ &= -1 \cdot 30 + 2 \cdot 18 \\ &= -1 \cdot 30 + 2(48 - 1 \cdot 30) \\ &= 2 \cdot 48 - 3 \cdot 30 \\ &= 2 \cdot 48 - 3(270 - 5 \cdot 48) \\ &= -3 \cdot 270 + 17 \cdot 48 \end{aligned}$$

Hieruit halen we een oplossing voor $48\ x + l\ 270 = 54$: uit $48 \cdot 17 - 3 \cdot 270 = 6$ volgt er $48 \cdot (17 \cdot 9) - (3 \cdot 9) \cdot 270 = 9 \cdot 6$. Daaruit volgt dat $x = 17 \cdot 9 = 153$ één van de gevraagde oplossingen is. Er zijn 6 verschillende oplossingen, telkens op afstand $270/6 = 45$ van de vorige oplossing. We schrijven alle oplossingen uit, met controle.

$$\begin{array}{rcr|rcrl} x = 153 & & & 48 \cdot 153 & = & 7344 & \equiv 54 \bmod 270 \\ x = 153 + 45 & \equiv & 198 & 48 \cdot 198 & = & 9504 & \equiv 54 \bmod 270 \\ x = 153 + 2 \cdot 45 & \equiv & 243 & 48 \cdot 243 & = & 11664 & \equiv 54 \bmod 270 \\ x = 153 + 3 \cdot 45 & \equiv & 18 & 48 \cdot 18 & = & 864 & \equiv 54 \bmod 270 \\ x = 153 + 4 \cdot 45 & \equiv & 63 & 48 \cdot 63 & = & 3024 & \equiv 54 \bmod 270 \\ x = 153 + 5 \cdot 45 & \equiv & 108 & 48 \cdot 108 & = & 5184 & \equiv 54 \bmod 270 \end{array}$$

Oefening 1

Wat gebeurt er nu als je in beide leden van de opgave een factor 6 wegdeelt? Los onderstaand probleem op, en vergelijk met bovenstaand antwoord. Zijn deze equivalent? Wat zegt stelling 5.15 hierover?
Los op in $\boldsymbol{Z}/_{270\boldsymbol{Z}}$*:* $13 \cdot x = 9$.

5.4 Chinese reststelling en oplossen van stelsels

$\boxed{x \equiv a_i \bmod m_i}$

De Chinese reststelling combineert het oplossen van aparte lineaire congruenties tot het oplossen van een stelsel lineaire congruenties. Dat wil zeggen dat alle oplossingen worden gezocht die tegelijkertijd aan 2 of meer lineaire congruenties voldoen. Deze methode werd ontdekt door de Chinese wiskundige Sun Zi, die leefde in de periode tussen 200 voor en 200 na Christus.

Stelling 5.16. Chinese reststelling *Als* $m_1, \ldots, m_n$ *paarsgewijs relatief priem zijn en groter dan 1, en* $a_1, \ldots, a_n \in \boldsymbol{Z}$*, dan is er een oplossing* x *voor het stelsel lineaire congruenties*

$$\begin{cases} x & \equiv & a_1 \ (mod\ m_1) \\ x & \equiv & a_2 \ (mod\ m_2) \\ & \ldots & \\ x & \equiv & a_n \ (mod\ m_n) \end{cases}$$

Als x *en* x' *beide oplossingen zijn, is* $x \equiv x' \ (mod\ M)$*, met* $M = m_1 m_2 \cdots m_n$.

Bewijs In plaats van enkel aan te tonen dát er een oplossing x bestaat, doen we iets méér in dit bewijs: we geven de constructie van de oplossing x. Het idee achter de oplossingsmethode gaat als volgt: het stelsel

$$\begin{cases} x & \equiv & a_1 \pmod{m_1} \\ x & \equiv & a_2 \pmod{m_2} \\ & \dots & \\ x & \equiv & a_n \pmod{m_n} \end{cases}$$

oplossen — waarbij voor elke congruentie eenzélfde x moet gevonden worden, is niet eenvoudig. Een opeenvolging van onafhankelijke congruenties oplossen, is dit echter wel:

$$\begin{array}{rcl} y_1 & \equiv & a_1 \pmod{m_1} \\ y_2 & \equiv & a_2 \pmod{m_2} \\ & \dots & \\ y_n & \equiv & a_n \pmod{m_n} \end{array}$$

We kunnen zelfs verderwerken met de onafhankelijke congruenties

$$\begin{array}{rcl} y_1 & \equiv & 1 \pmod{m_1} \\ y_2 & \equiv & 1 \pmod{m_2} \\ & \dots & \\ y_n & \equiv & 1 \pmod{m_n} \end{array}$$

We hebben het aanvankelijk moeilijke stelsel dus vervangen door n onafhankelijke eenvoudige voorwaarden. We zullen echter aantonen dat een oplossing $\{y_1, \dots, y_n\}$ van dit eenvoudige probleem, ons effectief een oplossing van het moeilijke probleem levert.

We merken eerst nog op dat de voorwaarde $y_1 \equiv 1 \pmod{m_1}$ nog steeds veel te veel oplossingen toelaat voor y_1. Dat is weinig werkbaar. Daarom eisen we nu ook dat y_1 veelvoud is van alle $m_i (i \neq 1)$. Of nog:

$$\begin{cases} y_1 & \equiv & 1 \pmod{m_1} \\ y_1 & \equiv & 0 \pmod{m_2} \\ & \dots & \\ y_1 & \equiv & 0 \pmod{m_{n-1}} \\ y_1 & \equiv & 0 \pmod{m_n} \end{cases} \text{ en } \begin{cases} y_2 & \equiv & 0 \pmod{m_1} \\ y_2 & \equiv & 1 \pmod{m_2} \\ & \dots & \\ y_2 & \equiv & 0 \pmod{m_{n-1}} \\ y_2 & \equiv & 0 \pmod{m_n} \end{cases} \dots \text{ en } \begin{cases} y_n & \equiv & 0 \pmod{m_1} \\ y_n & \equiv & 0 \pmod{m_2} \\ & \dots & \\ y_n & \equiv & 0 \pmod{m_{n-1}} \\ y_n & \equiv & 1 \pmod{m_n} \end{cases}$$

Als we dergelijke $(y_i)_{i=1 \to n}$ kunnen vinden, zien we makkelijk[3] dat $\sum a_i y_i$ voldoet aan het stelsel

$$\begin{cases} \sum a_i y_i & \equiv & a_1 \pmod{m_1} \\ \sum a_i y_i & \equiv & a_2 \pmod{m_2} \\ & \dots & \\ \sum a_i y_i & \equiv & a_{n-1} \pmod{m_{n-1}} \\ \sum a_i y_i & \equiv & a_n \pmod{m_n} \end{cases}$$

[3]Is dit geen eufemisme? In wetenschappelijke literatuur staat '*na enig rekenwerk vindt men*' steevast voor '*na 3 bladzijden rekenwerk vindt men*'. Dus toon aan dat de uitpsraak '$\sum a_i y_i$ *is oplossing*' volgt uit de conditie '*er bestaan dergelijke* y_i'.

met andere woorden, $x = \sum a_i y_i$ is (een van) de gezochte oplossing(en).

Rest ons dus y_1 (en $y_2, \ldots$) te vinden. De $n-1$ laatste regels van het stelsel voor y_1, drukken uit dat y_1 een veelvoud is van $m_2, m_3, \ldots, m_n$. Dus $y_1 = (\prod_{j \neq 1} m_j) \cdot l_1$, voor zekere l_1. Nu substitueren we dit in de eerste regel van het stelsel voor y_1 (die regel hadden we immers nog niet gebruikt).

$$(\prod_{j \neq 1} m_j) \cdot l_1 \equiv 1 \pmod{m_1}$$

Of anders genoteerd: zoek l_1 (en daaruit ook k_1) zodat

$$(\prod_{j \neq 1} m_j) \cdot l_1 + m_1 k_1 = 1.$$

Een oplossing voor deze Diophantische vergelijking in de onbekenden l_1 en k_1 is enkel te vinden als de grootste gemene deler $\text{ggd}((\prod_{j \neq 1} m_j), m_1)$ deler is van de constante in het rechterlid. Met andere woorden: l_1 bestaat als en slechts als $\text{ggd}((\prod_{j \neq 1} m_j), m_1) = 1$. Gelukkig is dat zo omwille van de voorwaarde waaronder de Chinese reststelling geldt. We hebben dus een oplossing voor l_1, waaruit ook de oplossing voor y_1 volgt. Een analoge redenering levert ons $y_2, \ldots, y_n$.

Aantonen dat $x \equiv x' \pmod{M}$ geldt, indien zowel x als x' oplossing zijn, kan als oefening. □

Voorbeeld

Het oorspronkelijk probleem van de Chinese wiskundige Sun Zi (of Sun Tsu) komt overeen met volgend stelsel:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

De oplossing is van de vorm $\sum a_i y_i$, met $y_i = l_i(\prod_{j \neq i} m_j)$. Met andere woorden

$$x = 2 \cdot l_1 \cdot 5 \cdot 7 + 3 \cdot l_2 \cdot 3 \cdot 7 + 2 \cdot l_3 \cdot 3 \cdot 5$$

Vullen we dit in in het linkerlid van elke congruentie, dan krijgen we hieruit drie aparte congruenties, die elk slechts één onbekende bevatten:

$$\begin{cases} 70\, l_1 \equiv 2 \pmod{3} \\ 63\, l_2 \equiv 3 \pmod{5} \\ 30\, l_3 \equiv 2 \pmod{7} \end{cases}$$

Dit komt overeen met

$$\begin{cases} 70 l_1 + k_1 3 = 2 \\ 63 l_2 + k_2 5 = 3 \\ 30 l_3 + k_3 7 = 2 \end{cases}$$

Gezien de waarde van k_i er voor onze oplossing niet toe doet, mogen we deze vervangen door een andere onbekende. Dit laat ons toe om de relatief grote getallen $(70, 63, 30)$ in de opgave kwijt te raken. Dit gaat als volgt:

$$\begin{array}{rl} & \left\{\begin{array}{rcl} 1l_1 + 69l_1 + 3k_1 & = & 2 \\ 3l_2 + 60l_2 + 5k_2 & = & 3 \\ 2l_3 + 28l_3 + 7k_3 & = & 2 \end{array}\right. \\ \Leftrightarrow & \left\{\begin{array}{rcl} 1l_1 + 3(23l_1 + k_1) & = & 2 \\ 3l_2 + 5(12l_2 + k_2) & = & 3 \\ 2l_3 + 7(4l_3 + k_3) & = & 2 \end{array}\right. \\ \Leftrightarrow & \left\{\begin{array}{rcl} 1l_1 + 3k_1' & = & 2 \\ 3l_2 + 5k_2' & = & 3 \\ 2l_3 + 7k_3' & = & 2 \end{array}\right. \\ \Leftrightarrow & \left\{\begin{array}{rcl} l_1 & \equiv & 2 \pmod 3 \\ 3l_2 & \equiv & 3 \pmod 5 \\ 2l_3 & \equiv & 2 \pmod 7 \end{array}\right. \end{array}$$

Merk op: uiteraard mag je in een oefening de tussenstappen (i.e. de notaties aan de hand van gelijkheidstekens in plaats van congruentietekens) overslaan, maar je moet wel goed voor ogen houden waar je mee bezig bent! Dus geen nieuwe rekenregeltjes vanbuiten leren, wel terugvallen op gekende wetten.

De laatst bekomen modulaire congruenties lossen we — indien niet op zicht — op met het algoritme van Euclides. Hier volgt echter onmiddellijk $l_1 = 2$, $l_2 = 1$, $l_3 = 1$. Een uitkomst van het stelsel is dus $x = 2 \cdot 2 \cdot 5 \cdot 7 + 3 \cdot 1 \cdot 3 \cdot 7 + 2 \cdot 1 \cdot 3 \cdot 5 = 233$; te herleiden tot de unieke uitkomst die in het gesloten interval $[0, M-1] = [0, 3 \cdot 5 \cdot 7 - 1] = [0, 104]$ thuishoort: $x = 23$. (Neem de proef op de som!)

Oefening 2

Los volgend stelsel op:

$$\left\{\begin{array}{rcl} x & \equiv & 1 \ (mod\ 5) \\ x & \equiv & 3 \ (mod\ 6) \\ x & \equiv & 0 \ (mod\ 7) \end{array}\right.$$

Oefening 3

Los volgend stelsel op:

$$\left\{\begin{array}{rcl} x & \equiv & 1 \ (mod\ 4) \\ x & \equiv & 3 \ (mod\ 5) \\ x & \equiv & 5 \ (mod\ 9) \end{array}\right.$$

Oefening 4

Los volgend stelsel op:

$$\left\{\begin{array}{rcl} x & \equiv & 1 \ (mod\ 6) \\ x & \equiv & 4 \ (mod\ 7) \\ x & \equiv & 7 \ (mod\ 9) \end{array}\right.$$

5.5 Residugetalsystemen: rekenen met grote getallen

Er doen zich twee problemen voor bij het rekenen met grote getallen. Enerzijds hebben we een fysische grens (`MAXINT`) die grote berekeningen in de weg staat. Anderzijds krijgen we bij bvb. optellen van zeer grote getallen tijdverlies omwille van 'overdracht' van cijfers / bits: eerst dienen de bits op de minst beduidende plaats opgeteld te worden, vóór de bits op de plaats er net links van opgeteld kunnen worden. Ze wachten namelijk op de overdracht van de bewerking die 'rechts van hen' gebeurde.

Om beide problemen op te lossen, voeren we een nieuw notatiesysteem voor getallen in, waarbij één grootheid (hoeveelheid) door verschillende getallen wordt gerepresenteerd. Elk van deze getallen op zich zal een vrij kleine hoeveelheid representeren, maar uit de combinatie van al deze getallen kan je toch eenduidig afleiden om welke oorspronkelijke grootheid het gaat. Hier komt de Chinese reststelling ons uiteraard te hulp: als we van een getal $\in \{0, 1, \ldots, M-1\}$ de moduli kennen genomen ten opzichte van $m_1, m_2, \ldots, m_n$ (met $\prod m_i = M$ en m_i onderling ondeelbaar), dan kennen we het getal zelf.

5.5.1 Voorstelling van getallen in residugetalsystemen

Omdat in de Chinese reststelling ondersteld wordt dat alle moduli m_i relatief priem zijn, nemen we voor m_i soms / gemakshalve priemmachten van verschillende priemgetallen. Omgekeerd, hebben we een getal m waarvan de priemfactorisatie gelijk is aan $\prod p_i^{\alpha_i}$, dan stellen we $m_i = p_i^{\alpha_i}$ (zodat $m = \prod m_i$) om de Chinese reststelling toe te passen. Let wel: dit wordt niet geëist in de premisses van de Chinese reststelling, maar het werkt handig voor het vervolg.

Stel $x \in \mathbb{Z}/_{m\mathbb{Z}}$, met $m = \prod p_i^{\alpha_i} = \prod m_i$ zoals hierboven, en

$$\begin{cases} x & \equiv & a_1 \pmod{m_1} \\ x & \equiv & a_2 \pmod{m_2} \\ & \cdots & \\ x & \equiv & a_k \pmod{m_k} \end{cases}$$

dan wordt het k-tal

$$\langle a_1, a_2, \ldots, a_k \rangle = \langle x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k \rangle$$

de **residurepresentatie** of **modulaire voorstelling** van x genoemd. Voor de eenvoud noteren we de residurepresentatie van x als

$$x \Leftrightarrow \langle x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k \rangle.$$

Merk op: deze modulaire voorstelling is uniek voor x, en x kan uit zijn modulaire voorstelling worden afgeleid, op een veelvoud van $m = \prod m_i$ na.

De modulaire voorstelling van x bestaat uit een k-tal elementen uit $\mathbb{Z}/_{m_i\mathbb{Z}}$, met m_i variabel. Dit leidt ons tot invoering van volgende definitie: de verzameling $(\mathbb{Z}/_{m\mathbb{Z}})^*$ is de 'direct

produkt-ontbinding' van $\boldsymbol{Z}/_{m\boldsymbol{Z}}$:

$$(\boldsymbol{Z}/_{m\boldsymbol{Z}})^* = \boldsymbol{Z}/_{m_1\boldsymbol{Z}} \times \boldsymbol{Z}/_{m_2\boldsymbol{Z}} \times \ldots \times \boldsymbol{Z}/_{m_k\boldsymbol{Z}}$$

met $m_i = p_i^{\alpha_i}$, en $\prod p_i^{\alpha_i}$ de priemfactorisatie van m.

Stelling 5.17. *De afbeelding $f : \boldsymbol{Z}/_{m\boldsymbol{Z}} \to (\boldsymbol{Z}/_{m\boldsymbol{Z}})^*$ die $x \in \boldsymbol{Z}/_{m\boldsymbol{Z}}$ afbeeldt op zijn modulaire voorstelling $\langle x \bmod m_1, \ldots, x \bmod m_k\rangle$ is een bijectie.*

Voorbeeld

Hieronder staan twee pogingen tot residurepresentatie van de 12 getallen in $\boldsymbol{Z}/_{12\boldsymbol{Z}}$. Geef het verschil aan; welke is zijn naam waardig?

0	$\Leftrightarrow$	$\langle 0,0\rangle$	4	$\Leftrightarrow$	$\langle 0,1\rangle$	8	$\Leftrightarrow$	$\langle 0,2\rangle$
1	$\Leftrightarrow$	$\langle 1,1\rangle$	5	$\Leftrightarrow$	$\langle 1,2\rangle$	9	$\Leftrightarrow$	$\langle 1,0\rangle$
2	$\Leftrightarrow$	$\langle 2,2\rangle$	6	$\Leftrightarrow$	$\langle 2,0\rangle$	10	$\Leftrightarrow$	$\langle 2,1\rangle$
3	$\Leftrightarrow$	$\langle 3,0\rangle$	7	$\Leftrightarrow$	$\langle 3,1\rangle$	11	$\Leftrightarrow$	$\langle 3,2\rangle$

versus

0	$\Leftrightarrow$	$\langle 0,0\rangle$	4	$\Leftrightarrow$	$\langle 0,4\rangle$	8	$\Leftrightarrow$	$\langle 0,2\rangle$
1	$\Leftrightarrow$	$\langle 1,1\rangle$	5	$\Leftrightarrow$	$\langle 1,5\rangle$	9	$\Leftrightarrow$	$\langle 1,3\rangle$
2	$\Leftrightarrow$	$\langle 0,2\rangle$	6	$\Leftrightarrow$	$\langle 0,0\rangle$	10	$\Leftrightarrow$	$\langle 0,4\rangle$
3	$\Leftrightarrow$	$\langle 1,3\rangle$	7	$\Leftrightarrow$	$\langle 1,1\rangle$	11	$\Leftrightarrow$	$\langle 1,5\rangle$

5.5.2 Rekenregels in residugetalsystsemen

Tellen we twee getallen $x, y \in \boldsymbol{Z}/_{m\boldsymbol{Z}}$ op, dan krijgen we voor de modulaire voorstelling van hun som:

$$\begin{aligned} x &\Leftrightarrow \langle x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k\rangle \\ y &\Leftrightarrow \langle y \bmod m_1, y \bmod m_2, \ldots, y \bmod m_k\rangle \\ x+y &\Leftrightarrow \langle (x+y) \bmod m_1, (x+y) \bmod m_2, \ldots, (x+y) \bmod m_k\rangle \\ &\quad = \langle (x \bmod m_1 + y \bmod m_1), (x \bmod m_2 + y \bmod m_2), \ldots, (x \bmod m_k + y \bmod m_k)\rangle \end{aligned}$$

Hieruit leiden we de enige zinnige definitie af voor de optelling van twee elementen van $(\boldsymbol{Z}/_{m\boldsymbol{Z}})^*$ (genoteerd aan de hand van de operator $+_m$):

$$\langle a_1, a_2, \ldots, a_k\rangle +_m \langle b_1, b_2, \ldots, b_k\rangle = \langle a_1 +_{m_1} b_2, a_2 +_{m_2} b_2, \ldots, a_k +_{m_k} b_k\rangle$$

waarbij $+_{m_i}$ staat voor 'optelling in $\boldsymbol{Z}/_{m_i\boldsymbol{Z}}$' (dus modulo m_i).

Analoog vinden we de enige zinnige definitie voor de vermenigvuldiging van twee elementen van $(\boldsymbol{Z}/_{m\boldsymbol{Z}})^*$ (genoteerd aan de hand van de operator $\cdot_m$):

$$\langle a_1, a_2, \ldots, a_k\rangle \cdot_m \langle b_1, b_2, \ldots, b_k\rangle = \langle a_1 \cdot_{m_1} b_2, a_2 \cdot_{m_2} b_2, \ldots, a_k \cdot_{m_k} b_k\rangle$$

waarbij $\cdot_{m_i}$ staat voor 'vermenigvuldiging in $\boldsymbol{Z}/_{m_i\boldsymbol{Z}}$' (dus modulo m_i).

We zien dat de bewerkingen $+_m, -_m$ en $\cdot_m$ in $\boldsymbol{Z}/_{m\boldsymbol{Z}}$ uitgevoerd kunnen worden in $(\boldsymbol{Z}/_{m\boldsymbol{Z}})^*$ door de overeenkomstige bewerkingen $+_{m_i}$, $-_{m_i}$ en $\cdot_{m_i}$ in $\boldsymbol{Z}/_{m_i\boldsymbol{Z}}$.

5.5.3 Toepassing: rekenen met grote getallen

Uit dit alles volgt een methode om het tijdrovend rekenen met grote getallen op te splitsen in handzamer problemen. Hebben we twee zeer grote getallen x en y, te groot om voor te stellen in één variabele, dan bewaren we hun modulaire voorstellingen $\langle a_1, a_2, \ldots, a_k \rangle$ en $\langle b_1, b_2, \ldots, b_k \rangle$ in telkens k variabelen. Willen we bewerkingen $(+, -, \cdot)$ loslaten op x en y, dan passen we deze bewerkingen toe op alle $2k$ variabelen afzonderlijk.

Voordelen

- We hoeven van de (tussen)uitkomsten slechts de waarde modulo m_i te bewaren.
- De beginvariabelen zijn kleiner, zodat er niet te lang op de 'carry' (=overdracht) gewacht moet worden.
- Er kunnen k berekeningen simultaan gebeuren — onafhankelijk van elkaar.

Uiteraard zal er slechts teruggerekend worden naar $\boldsymbol{Z}/_{m\boldsymbol{Z}}$ op het moment dat álle bewerkingen en tussenuitkomsten verwerkt zijn in $(\boldsymbol{Z}/_{m\boldsymbol{Z}})^*$.

Voorbeeld

Bereken $z = x + y = 12345 + 23456$ op een computer die maximaal getalwaarde 100 kan voorstellen.

We maken eerst een ruwe schatting voor de uitkomst, zodat we weten in welke verzameling $\boldsymbol{Z}/_{m\boldsymbol{Z}}$ deze uitkomst nog kan geschreven worden — zonder 'overflow' te genereren. Gezien $10.000 + 30.000 = 40.000$, moet $m \approx 40.000$. We zoeken een aantal grote getallen, kleiner dan 100, die onderling ondeelbaar zijn en zo dat hun product ongeveer gelijk is aan 40.000. De getallen $m_1 = 99$ en $m_2 = 98$ voldoen samen niet, nemen we er $m_3 = 97$ bij, dan voldoet de verzameling $\{m_1, m_2, m_3\}$ wel. We berekenen:

$$\begin{cases} 12345 &= 69 \bmod 99 \\ 12345 &= 95 \bmod 98 \\ 12345 &= 26 \bmod 97 \end{cases} \quad \text{en} \quad \begin{cases} 23456 &= 92 \bmod 99 \\ 23456 &= 34 \bmod 98 \\ 23456 &= 79 \bmod 97 \end{cases}$$

Daaruit volgt

$$\begin{cases} z &= 62 \bmod 99 \\ z &= 31 \bmod 98 \\ z &= 8 \bmod 97 \end{cases}$$

Uit de Chinese reststelling volgt dan

$$z = 62 \cdot l_1 \cdot 98 \cdot 97 + 31 \cdot l_2 \cdot 99 \cdot 97 + 8 \cdot l_3 \cdot 99 \cdot 98$$

Invullen van deze uitdrukking voor z in het laatste stelsel, geeft ons

$$\begin{cases} 62 \cdot 98 \cdot 97 \quad l_1 &= 62 \bmod 99 \\ 31 \cdot 99 \cdot 97 \quad l_2 &= 31 \bmod 98 \\ 8 \cdot 99 \cdot 98 \quad l_3 &= 8 \bmod 97 \end{cases}$$

Vermijden we zoveel mogelijk rekenwerk (lees: grote getallen) aan de hand van de redenering die reeds aan bod kwam op blz 88, dan komt er:

$$
\begin{aligned}
&\Leftrightarrow \left\{ \begin{array}{rrcl} 62(99-1)(99-2) & l_1 & = & 62 \bmod 99 \\ 31(98+1)(98-1) & l_2 & = & 31 \bmod 98 \\ 8(97+2)(97+1) & l_3 & = & 8 \bmod 97 \end{array} \right. \\
&\Leftrightarrow \left\{ \begin{array}{rrcl} 62(-1)(-2) & l_1 & = & 62 \bmod 99 \\ 31(1)(-1) & l_2 & = & 31 \bmod 98 \\ 8(2)(1) & l_3 & = & 8 \bmod 97 \end{array} \right. \\
&\Leftrightarrow \left\{ \begin{array}{rrcl} 124 & l_1 & = & 62 \bmod 99 \\ -31 & l_2 & = & 31 \bmod 98 \\ 16 & l_3 & = & 8 \bmod 97 \end{array} \right. \\
&\Leftrightarrow \left\{ \begin{array}{rrcl} 25 & l_1 & = & 62 \bmod 99 \\ 67 & l_2 & = & 31 \bmod 98 \\ 16 & l_3 & = & 8 \bmod 97 \end{array} \right. \\
&\Leftrightarrow \left\{ \begin{array}{rrcl} 25\, l_1 + k_1\, 99 & & = & 62 \\ 67\, l_2 + k_2\, 98 & & = & 31 \\ 16\, l_3 + k_3\, 97 & & = & 8 \end{array} \right.
\end{aligned}
$$

We lossen deze drie congruenties op adhv het algoritme van Euclides (of op zicht):

$25\, l_1 + k_1\, 99 = 62$	$67\, l_2 + k_2\, 98 = 31$	$16\, l_3 + k_3\, 97 = 8$
$99 = 3 \cdot 25 + 24$ $25 = 1 \cdot 24 + 1$	$98 = 1 \cdot 67 + 31$	$97 = 6 \cdot 16 + 1$
$1 = 25 - 1 \cdot 24$ $= 25 - 1 \cdot (99 - 3 \cdot 25)$ $= -1 \cdot 99 + 4 \cdot 25$		$1 = 1 \cdot 97 - 6 \cdot 16$
$\Rightarrow l_1 = 4 \cdot 62 \bmod 99$ $= 50 \bmod 99$	$\Rightarrow l_2 = -1 \bmod 98$	$\Rightarrow l_3 = -6 \cdot 8 \bmod 97$ $= -48 \bmod 97$

Dit invullen in de uitdrukking voor z geeft $z = 25.445.339 \bmod (99 \cdot 98 \cdot 97) = 35.801 \bmod 941.094$. Dit komt overeen met de verwachte waarde: 12.345+23.456 = 35.801.

Zoals reeds aangegeven, omzeilen we met het rekenen in een residugetalsysteem twee belangrijke nadelen van het gewone (binair geprogrammeerde) optellen in $\boldsymbol{Z}$ (of $\boldsymbol{Z}/_{m\boldsymbol{Z}}$, met m de maximale getalwaarde die voorgesteld kan worden).

Enerzijds moet er niet gewacht worden op de overdracht van de minderbeduidende digit naar de volgende; anderzijds is elke m_i beduidend kleiner dan m, zodat berekeningen in $\boldsymbol{Z}/_{m_i\boldsymbol{Z}}$ eenvoudiger zullen zijn dan in $\boldsymbol{Z}/_{m\boldsymbol{Z}}$. Dit is het principe waarop de werking van de residucomputer gebaseerd is, een speciaal type van highspeed computer, met belangrijke toepassingen in onder andere beeld- en signaalverwerking.

Hoofdstuk 6

Diophantische vergelijkingen: niet-lineair

We zagen dat $\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot$ een commutatieve ring met eenheidselement is (n niet per se priem), en $\mathbb{Z}/_{p\mathbb{Z}}, +, \cdot$ een veld (p priem). Dit wil zeggen dat optelling, aftrekking, vermenigvuldiging én deling (dat laatste voor $\mathbb{Z}/_{p\mathbb{Z}}$) goed gedefinieerd zijn. De volgende bewerking in het rijtje is de machtsverheffing. Gezien de vermenigvuldiging altijd mogelijk is, is de machtsverheffing dat ook. Maar is de inverse bewerking, de logaritme dat wel? Gegeven $a, b \in \mathbb{Z}/_{n\mathbb{Z}}$, is er dan altijd een x te vinden zodat $a^x = b \bmod n$? We bespreken eerst een aantal speciale gelijkheden, die ons van pas kunnen komen.

6.1 Kleine stelling van Fermat en oplossen van $\boxed{x \equiv a^b \bmod n}$

Vóór we een stelling uit de kast trekken omtrent machten in $\mathbb{Z}/_{n\mathbb{Z}}$, loont het de moeite om zelf eens op onderzoek te gaan naar eigenschappen van die machten. Neem bijlage E ter hand. Hier vind je voor elke commutatieve ring $\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot$ ($n \in [4, 17]$) een opsomming van alle elementen met hun opeenvolgende machten. Reken zelf 2 tabellen na. Merk op: je hebt nooit grote getallen nodig. Je berekent 3^5 aan de hand van 3^4, waarvan je de gereduceerde waarde terugvindt in de tabel.

Als je enkel de tabellen van $\mathbb{Z}/_{p\mathbb{Z}}$ bekijkt (dus $\mathbb{Z}/_{5\mathbb{Z}}$, $\mathbb{Z}/_{7\mathbb{Z}}$,$\mathbb{Z}/_{11\mathbb{Z}}$, $\mathbb{Z}/_{13\mathbb{Z}}$, $\mathbb{Z}/_{17\mathbb{Z}}$), dan zou het je moeten opvallen: een kolom met allemaal ééntjes. Dit is ook wat Fermat was opgevallen, vandaar volgende stelling:

Stelling 6.1. Kleine stelling van Fermat
Stel a een positief geheel getal, en p priem. Dan geldt er

$$\boxed{a^{p-1} \equiv 1 \ (mod\ p) \qquad als\ ggd(a, p) = 1}$$

Bewijs De residu's modulo p van $a, 2a, 3a, \ldots, (p-1)a$ zijn alle verschillend. (Inderdaad, stel $ia \equiv ja \pmod{p}$ met $i \neq j$. Dan is $(i-j)a \equiv 0 \pmod{p}$ met $(i-j) \neq 0$. Daaruit volgt dat p ofwel a deelt, ofwel $(i-j)$. De eerste uitspraak is onmogelijk, gezien a en p onderling priem zijn. De tweede uitspraak is onmogelijk, gezien $i \neq j$ en beide kleiner zijn dan p.) We kunnen de residus dus gelijkstellen aan $1, 2, \ldots, p-1$ in één of andere volgorde. Alle residu's vermenigvuldigen geeft:

$$\begin{array}{rrcl} & a \cdot 2a \cdot \ldots \cdot (p-1)a & \equiv & [(a \bmod p) \cdot (2a \bmod p) \cdot \ldots \cdot ((p-1)a \bmod p)] \bmod p \\ & & \equiv & 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p} \\ & & \equiv & (p-1)! \pmod{p} \\ \Rightarrow & (p-1)!a^{p-1} & \equiv & (p-1)! \pmod{p} \\ {\scriptstyle p \text{ priem}} \Rightarrow & a^{p-1} & \equiv & 1 \bmod p \end{array}$$

Merk op: de laatste stap mag uitgevoerd worden omdat $(p-1)!$ niet deelbaar is door p. □

Waarschuwing Bovenstaande stelling is van bedrieglijke eenvoud - en een ideale test om na te gaan of je de draagweidte van één en ander ten volle beseft. Toch werd ervoor gekozen om niet in het bewijs zelf in te grijpen (je vindt het ook zó terug in vakliteratuur), maar deze tips wil ik je niet onthouden:

Tip 1 Om deze stelling opnieuw te kunnen opstellen, heb je een kapstok nodig. Je moet weten dat je de residu's $\{a, 2a, \ldots, (p-1)a\}$ moet beschouwen. Maak hiervoor een tekening: de verzameling $\boldsymbol{Z}/_{p\boldsymbol{Z}}$ van congruentieklassen $\{[0], [1], \ldots, [p-1]\}$ en (diezelfde) verzameling $\boldsymbol{Z}/_{p\boldsymbol{Z}}$ van congruentieklassen $\{[0], [a], \ldots, [(p-1)a]\}$. Je start dan uiteraard met aantonen dat er in die tweede voorstelling geen dubbele elementen zitten.

Tip 2 Waar heb je gebruik gemaakt van de voorwaarden waaronder de stelling geldt (te weten: p priem, $\text{ggd}(a, p) = 1$)? Als je die nergens gebruikt, heb je een *nog sterkere* stelling bewezen. Knap staaltje – maar ben je wel zeker van je stuk?

Tip 3 Áls je de voorwaarde (bvb p priem) ingeroepen hebt om een welbepaalde stap in je bewijs te zetten, kon je die stap dan níet zetten voor het tegendeel van de voorwaarde (bvb p niet priem)? Ga hier niet te licht over – toon aan!

Stelling 6.2. *Stel a een positief geheel getal, en p priem. Dan geldt er*

$$a^p \equiv a \ (mod\ p).$$

Bewijs Merk op: nu staat er geen beperking op a. Indien $\text{ggd}(a, p) = 1$ volgt de gelijkheid direct uit voorgaande stelling. Indien $\text{ggd}(a, p) \neq 1$ is $p \mid a$. Dus $a^p \equiv 0 \equiv a \pmod{p}$. □

Stelling 6.3. Stelling van Euler
Stel a en n positieve gehele getallen. Dan geldt er

$$a^{\phi(n)} \equiv 1 \ (mod\ n) \qquad als\ ggd(a, n) = 1$$

Bewijs Merk op: n is hier niet per se priem. Het bewijs is analoog aan dat van de stelling van Fermat. Nu beschouw je enkel de residuklassen $r_1, r_2, \ldots, r_{\phi(n)}$ waarvoor r_i relatief priem is met n. De veelvouden van deze residuklassen $ar_1, ar_2, \ldots, ar_{\phi(n)}$ zijn dan onderling ook verschillend, en ar_i is nog steeds relatief priem met n. Dus is de verzameling $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ gelijk aan de verzameling $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ in $\mathbb{Z}/_{n\mathbb{Z}}$. Daaruit:

$$\begin{aligned} & (ar_1)(ar_2)\ldots(ar_{\phi(n)}) \equiv r_1 r_2 \ldots r_{\phi(n)} \pmod{n} \\ \Leftrightarrow \quad & a^{\phi(n)} r_1 r_2 \ldots r_{\phi(n)} \equiv r_1 r_2 \ldots r_{\phi(n)} \pmod{n} \end{aligned}$$

Omdat elke r_i relatief priem is met n, mogen deze factoren weggedeeld worden, waaruit $a^{\phi(n)} \equiv 1 \pmod{n}$.

Oefening 1

Bereken de rest na deling van 4^{35} *door* 17.

Oefening 2

Bereken 10^{1803} *(mod* 693*).*

Oefening 3

Bereken 25^{98} *(mod* 168*).*

Oefening 4

Bereken 7^{2006} *(mod* 23*).*

Oefening 5

Neem bijlage E erbij, en duid aan waar je de kleine stelling van Fermat terugvindt. Idem voor de stelling van Euler.

6.2 Discrete logaritmen en oplossen van $\boxed{a^x \equiv b \bmod n}$

Na de eenvoudige lineaire Diophantische vergelijkingen uit vorig hoofdstuk, zoeken we nu oplossingen voor ingewikkelder vergelijkingen. Stel dat a gegeven is, en je zoekt x zo dat

$$a^x \equiv 1 \bmod n.$$

Uit de stelling van Euler weten we dat voor a en n relatief priem, er zeker een getal x bestaat dat aan deze congruentie voldoet, namelijk $x = \phi(n)$. Want

$$a^{\phi(n)} \equiv 1 \bmod n.$$

Het zou echter kunnen dat er nog kleinere getallen x bestaan, waarvoor $a^x \equiv 1 \bmod n$. (Zoek voorbeelden in bijlage E!)

Definitie. *De kleinste positieve exponent x waarvoor $a^x \equiv 1$ mod n noemen we*

- *de orde van a modulo n*
- *de exponent waartoe a behoort*
- *de lengte van de periode gegenereerd door a*

Een voorbeeld om dit te verduidelijken:

$$\begin{aligned} 9^1 &\equiv 9 \bmod 13 \\ 9^2 &\equiv 3 \bmod 13 \\ 9^3 &= 27 \equiv 1 \bmod 13 \\ 9^4 &\equiv 9 \bmod 13 \\ 9^5 &\equiv 3 \bmod 13 \end{aligned}$$

We moeten niet verder zoeken: een macht van 9 zal in $\mathbb{Z}/_{13\mathbb{Z}}$ enkel 3, 9 of 1 als uitkomst hebben. Elke twee machten van 9 wier exponenten een veelvoud van 3 van elkaar verschillen, zijn congruent in $\mathbb{Z}/_{13\mathbb{Z}}$. De reeks $(9^i)_{i \in \mathbb{N}}$ is periodisch met lengte 3: de kleinste positieve exponent x zodat $9^x \equiv 1 \bmod 13$.

Schrijven we alle machten (tot de 12^e) van alle getallen in $\mathbb{Z}/_{13\mathbb{Z}}$ uit, dan krijgen we volgend overzicht.

lengte van periode	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
1	**1**	1	1	1	1	1	1	1	1	1	1	1
12	**2**	**4**	**8**	**3**	**6**	**12**	**11**	**9**	**5**	**10**	**7**	**1**
3	**3**	**9**	**1**	3	9	1	3	9	1	3	9	1
6	**4**	**3**	**12**	**9**	**10**	**1**	4	3	12	9	10	1
4	**5**	**12**	**8**	**1**	5	12	8	1	5	12	8	1
12	**6**	**10**	**8**	**9**	**2**	**12**	**7**	**3**	**5**	**4**	**11**	**1**
12	**7**	**10**	**5**	**9**	**11**	**12**	**6**	**3**	**8**	**4**	**2**	**1**
4	**8**	**12**	**5**	**1**	8	12	5	1	8	12	5	1
3	**9**	**3**	**1**	9	3	1	9	3	1	9	3	1
6	**10**	**9**	**12**	**3**	**4**	**1**	10	9	12	3	4	1
12	**11**	**4**	**5**	**3**	**7**	**12**	**2**	**9**	**8**	**10**	**6**	**1**
2	**12**	**1**	12	1	12	1	12	1	12	1	12	1

Je kan de periode van elke reeks $(a^i)_{i\in\mathbb{N}}$ aflezen uit de tabel: de periode eindigt altijd op 1. Merk op dat de lengte van een periode altijd een deler van $\phi(13) = 12$ is. Sommige periodes beslaan de hele tabel, en bevatten dus alle (niet-nul) getallen van $\boldsymbol{Z}/_{p\boldsymbol{Z}}$. We noemen het basisgetal a dan een **primitieve wortel van de modulus** p. Voor p priem, genereert de primitieve wortel via machtsverheffing alle getallen van $\boldsymbol{Z}/_{p\boldsymbol{Z}}$ (behalve nul). Voor $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ is dit niet het geval, maar zal een primitieve wortel van de modulus n via machtsverheffing zoveel mogelijk (i.e. $\phi(n)$) verschillende getallen genereren.

Definitie. *Elk getal dat van de orde $\phi(m)$ is (en dat is de hoogst mogelijke orde die er bestaat), is een primitieve wortel van m. De reeks*

$$a, a^2, a^3, \ldots, a^{\phi(m)}$$

bestaat dan uit $\phi(m)$ verschillende getallen, die allemaal relatief priem zijn ten opzichte van m.

Voor p een priemgetal:

$$a, a^2, a^3, \ldots, a^{p-1}$$

zijn alle verschillend als en slechts als a een primitieve wortel is van p.[1]

De primitieve wortels van 13 zijn 2, 6, 7 en 11. Niet alle gehele getallen hebben primitieve wortels. Men kan aantonen dat de enige getallen die primitieve wortels hebben, van de volgende vorm zijn:

$$2, 4, p^\alpha \text{ en } 2p^\alpha \qquad (p \text{ een oneven priemgetal, } \alpha \geq 1)$$

[1] Merk op: in het bewijs van de kleine stelling van Fermat toonden we aan dat $a, 2a, \ldots, (p-1)a$ alle verschillend zijn, voor p priem en a willekeurig. Voor de hier geciteerde eigenschap van de machten $a, a^2, \ldots$ moet a echter een primitieve wortel van de modulus p zijn!

6.2.1 Rekenregels voor discrete logaritmen

Rekenregels voor optelling, aftrekking, vermenigvuldiging, deling in $\boldsymbol{Z}/_{m\boldsymbol{Z}}$ waren analoog aan de overeenkomstige bewerkingen in $\boldsymbol{Z}$. Geldt dit ook voor de discrete logaritmen?

In $\boldsymbol{Z}$ hebben we:

$$\begin{array}{lllll} (1) & \log_a(a^x) & = & x \qquad \text{of} & a^{\log_a(x)} = x \\ (2) & \log_a(1) & = & 0 & \\ (3) & \log_a(a) & = & 1 & \\ (4) & \log_a(xy) & = & \log_a(x) + \log_a(y) & \\ (5) & \log_a(x^r) & = & r \log_a(x) & \end{array}$$

Gegeven een primitieve wortel a van een getal p. Stel dat $b \equiv a^i \bmod p$, dan noemen we i de **index van het getal** b **voor de basis** a **mod** p. We noteren dit als $\text{ind}_{a,p}(b)$. Merk op: deze index geeft dus het rangnummer mee van b's plaats in de periode van a.

Het analogon van de vijf genoemde eigenschappen:

(1) $a^{\text{ind}_{a,p}(x)} = x$.

(2) $\text{ind}_{a,p}(1) = 0$, want $a^0 \bmod p = 1 \bmod p = 1$.

(3) $\text{ind}_{a,p}(a) = 1$, want $a^1 \bmod p = a$.

(4) We kunnen aantonen dat een dergelijke rekenregel ook hier geldt; maar dan wel modulo $\phi(p)$ genomen.
$\text{ind}_{a,p}(xy) = (\text{ind}_{a,p}(x) + \text{ind}_{a,p}(y)) \bmod \phi(p)$.

(5) Bij inductie uit vorige eigenschap:
$\text{ind}_{a,p}(x^r) = (r \ \text{ind}_{a,p}(x)) \bmod \phi(p)$.

Voorbeeld

We weten uit voorgaande tabel dat 13 precies 4 primitieve wortels heeft, nl. 2, 6, 7 en 11. We kunnen dus van elk getal in $\boldsymbol{Z}/_{13\boldsymbol{Z}}$ de logaritme berekenen ten opzichte van basis 2, 6, 7 of 11. (Dit is: we kunnen de index / plaats bepalen waar x zich bevindt in de periode van de basis.)

Discrete logaritme met basis 2, modulo 13:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_{2,13}(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Discrete logaritme met basis 6, modulo 13:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_{6,13}(a)$	12	5	8	10	9	1	7	3	4	2	11	6

Merk op: $\text{ind}_{2,13}(5 \cdot 7) = \text{ind}_{2,13}(35) = \text{ind}_{2,13}(35 - 2 \cdot 13) = \text{ind}_{2,13}(9) = 8$, terwijl $\text{ind}_{2,13}(5) + \text{ind}_{2,13}(7) = 9 + 11 = 20$. Waaruit rekenregel (4) nogmaals blijkt: $\text{ind}_{2,13}(5 \cdot 7) = (\text{ind}_{2,13}(5) + \text{ind}_{2,13}(7)) \bmod 12$. Het gaat hier dus wel degelijk om een berekening modulo $12 = \phi(13)$, en niet om modulo 13.

We stelden nu een paar tabellen op om de discrete logaritme $\text{ind}_{a,p}(x)$ van x ten opzichte van de basis a modulo p te berekenen. Dit is uiteraard een weinig elegante manier om de discrete logaritme van een getal te zoeken. Er bestaan methodes die het zoekwerk wat versnellen, maar het blijft zoekwerk. Lees- en programmeertip: het algoritme met naam *baby step - giant step*. In ieder geval kom je discrete logaritmen tegen in de cursus beveiliging, precies omdat de berekening ervan niet evident is.

Oefening 6

Beantwoord volgende vragen zó dat een niet-ingewijde het begrip primitieve wortel *kan vatten.*
Toon aan dat 6 slechts 1 primitieve wortel bezit (bepaal deze en leg uit). Noem die primitieve wortel a. Kunnen we nu $a^x \equiv b \bmod 6$ in elk geval ($\forall b$) oplossen naar x? Waarom wel of niet?

Oefening 7

Toon aan dat 12 geen primitieve wortels heeft.

Oefening 8

De orde van b modulo a noteren we als $\text{ord}_a b$. (Let op: we hebben het hier over de orde*, niet over de* index*.) Geef eerst aan wat de* orde *van een element betekent, en leg uit wat dit te maken heeft met* primitieve wortels*.*
Bepaal onderstaande ordes, en geef aan of b een primitieve wortel is van a (en waarom).

1. $ord_5 2$
2. $ord_{10} 3$
3. $ord_{13} 10$
4. $ord_{10} 7$

Samenvatting van hoofdstuk 5 en 6

Controleer nu voor jezelf. Gegeven 4 variabelen, waarvan er telkens 1 onbekend is. Kan je dan onderstaande $4 \cdot 3 = 12$ congruenties oplossen? Welke rekenregels of stellingen zou je nodig kunnen hebben? Probeer eventueel met (grote) getallen!

1. $(a + b) \bmod c \equiv e$
2. $(ab) \bmod c \equiv e$
3. $(a^b) \bmod c \equiv e$

Hoofdstuk 7

Eindige velden

7.1 Constructie van eindige velden

In vorige hoofdstukken zagen we dat elke verzameling $\mathbb{Z}/_{p\mathbb{Z}}$ met de bewerkingen + en $\times$ een veld vormen. We vonden dus een eindige verzameling met mooie eigenschappen voor optelling en vermenigvuldiging. Eindige verzamelingen interesseren ons, omdat software in se bestaat uit een eindige reeks nullen en enen. Stel dat we die reeksen opdelen in groepjes van 1 bit, dan werken we dus met 2 verschillende elementen, of met de verzameling $\mathbb{Z}/_{2\mathbb{Z}}$. Dit is echter amper bruikbaar. Groeperen we de bits in groepjes van 8 (of 16 of 25 of 32 of...) dan werken we dus met 2^8 (of 2^{16} of 2^{25} of...) verschillende elementen. Probleem: de gekende verzameling van 2^8 elementen is $\mathbb{Z}/_{2^8\mathbb{Z}}$, maar dat is geen veld. We gaan dus op zoek naar een veld van 2^8 elementen. Of nog: we zoeken een manier om optelling en vermenigvuldiging te definiëren op een verzameling van 2^8 verschillende elementen, zodat alle eigenschappen van een veld voldaan zijn. Uiteraard zullen we niet enkel zoeken naar dit specifieke veld, maar meteen naar het algemene geval: een veld van de orde p^k met p priem en $k > 1$.

Daarvoor keren we even terug naar hoofdstuk 1, waar we de uitbreiding zagen van $\mathbb{N}$ naar $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$. De uitbreiding naar $\mathbb{Q}$ en $\mathbb{R}$ levert ons niets dat navolging verdient: we willen vooral niet dat er tussen 2 bestaande elementen plots een oneindig aantal elementen toegevoegd wordt. Maar misschien levert de uitbreiding naar $\mathbb{C}$ ons iets op? Vertrek van de getallenas van $\mathbb{Z}$. De uitbreiding tot het complexe vlak zou dan een (oneindige) verzameling van rasterpunten $a + bi$ geven, met $a, b \in \mathbb{Z}$ en $i^2 = -1$. Merk op: de imaginaire eenheid i is een (in $\mathbb{Z}$ ongekend) element dat de oplossing is van de vierkantsvergelijking $x^2 + 1 = 0$ die in $\mathbb{Z}$ geen oplossingen heeft.

Nadeel van deze werkwijze: we vertrokken van $\mathbb{Z}$, dus is de geconstrueerde verzameling ook oneindig. Vertrekken we daarentegen van de eindige verzameling $\mathbb{Z}/_{5\mathbb{Z}}$, dan bevat de verzameling $\{a+b\alpha \mid \alpha \text{ imaginair getal en } a, b \in \mathbb{Z}/_{5\mathbb{Z}}\}$ precies 25 punten. We voegen dus, naast de reële dimensie, een imaginaire (of denkbeeldige) dimensie toe. De éénheid van deze imaginaire dimensie noemen we α, en zou de oplossing moeten zijn van een vierkantsvergelijking die in $\mathbb{Z}/_{5\mathbb{Z}}$ geen oplossing heeft. Ga de 5 elementen van $\mathbb{Z}/_{5\mathbb{Z}}$ af: blijkbaar is elk kwadraat gelijk aan $0, 1$ of -1. Dus zijn $x^2 + 2$ en $x^2 - 2$ vergelijkingen zonder oplossingen. Nemen

we α met $\alpha^2 = 2$ (of $\alpha^2 - 2 = 0$), dan is α een goede kandidaat voor de imaginaire éénheid. We hebben dus een verzameling van 25 elementen, die we noteren als $\{a + b\alpha \mid \alpha^2 = 2 \text{ en } a, b \in \mathbb{Z}/_{5\mathbb{Z}}\}$.

Toepasselijker voor bits en bytes: we kunnen $\mathbb{Z}/_{2\mathbb{Z}}$ uitbreiden tot een verzameling van 4 elementen, nl. $\{0, 1, \alpha, \alpha+1\}$ waarbij α een oplossing is van een vierkantsvergelijking die geen oplossing heeft in $\mathbb{Z}/_{2\mathbb{Z}} = \{0, 1\}$. Er zijn slechts 4 vierkantsvergelijkingen in $\mathbb{Z}/_{2\mathbb{Z}}$ (dit is een tel-oefening, zie hoofdstuk 3), nl. $x^2 = 0$, $x^2 + 1 = 0$, $x^2 + x = 0$ en $x^2 + x + 1 = 0$. De eerste drie hebben een oplossing in $\mathbb{Z}/_{2\mathbb{Z}}$, de laatste heeft dit niet. Dus is α het *imaginaire* getal waarvoor geldt $\alpha^2 + \alpha + 1 = 0$. Werk hieronder de optellings- en vermenigvuldigingstabel voor deze verzameling $\{0, 1, \alpha, \alpha+1\}$ uit. (Tussenstappen doe je in het klad, schrijf enkel het eindresultaat.)

$+$	0	1	α	$1+\alpha$
0				
1				
α				
$1+\alpha$				

$\times$	0	1	α	$1+\alpha$
0				
1				
α				
$1+\alpha$				

Merk op: telkens je α^2 tegenkomt, vervang je dit door de uitdrukking $\alpha+1$, want $\alpha^2+\alpha+1 = 0 \Leftrightarrow \alpha^2 = -\alpha - 1 \Leftrightarrow \alpha^2 = \alpha + 1$ (coëfficiënten in $\mathbb{Z}/_{2\mathbb{Z}}$!). Als je deze optellings- en vermenigvuldigingstabellen vergelijkt met die van $\mathbb{Z}/_{4\mathbb{Z}}$ zou je moeten opvallen dat de nieuwe verzameling geen nuldelers meer heeft! (Je vindt geen getallen a, b verschillend van 0 waarvoor $a \times b = 0$.)

Kunnen we dit nu doortrekken? Kunnen we nu imaginaire éénheden blijven verzinnen, zodat we naast de reële en de imaginaire α-as nog een β-as kunnen toevoegen? Dan zou elk element bepaald worden door 3 getallen uit $\mathbb{Z}/_{p\mathbb{Z}}$, en hebben we $p \cdot p \cdot p = p^3$ elementen. De truc (zeg maar deus ex machina) bestaat er nu in om geen totaal nieuwe, onafhankelijke imaginaire éénheid β op te dissen, maar een getal α te zoeken dat oplossing is van een derdegraadsvergelijking die geen oplossingen heeft in $\mathbb{Z}/_{p\mathbb{Z}}$, en dan α en α^2 als twee (verschillende) imaginaire eenheden te nemen. De p^3 elementen uit onze nieuwe verzameling worden dan genoteerd als $a_0 + a_1\alpha + a_2\alpha^2$ met $a_i \in \mathbb{Z}/_{p\mathbb{Z}}$.

Om aan te tonen dat we inderdaad met een veld te maken hebben (nl. dat optelling en vermenigvuldiging voldoen aan de nodige voorwaarden), hoeven we maar de optelling en vermenigvuldiging goed te definiëren, en deze definitie dan te onderzoeken op hun eigenschappen (zie bijlage D).

Notatie van een element Elk element uit de verzameling van p^k elementen, noteren we aan de hand van een k-tuple $(a_0, a_1, \ldots, a_{k-1})$ met $a_i \in \mathbb{Z}/_{p\mathbb{Z}}$, of nog als $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{k-1}a^{k-1}$ met α de wortel van een k-demachtsvergelijking die geen oplossing heeft in $\mathbb{Z}/_{p\mathbb{Z}}$. De getallen a_i kunnen we ook de coördinaten van het getal noemen ten opzichte van de basis $(1, \alpha, \alpha^2, \ldots, \alpha^{k-1})$.

Optelling Optellen gebeurt zoals in $\mathbb{C}$: overeenkomstige coördinaten worden opgeteld. Daarbij gelden de rekenregels van $\mathbb{Z}/_{p\mathbb{Z}}$, dus er wordt modulo p gerekend.

Vermenigvuldiging Hier gebruiken we bij voorkeur de veeltermnotatie. Stel $a = \sum_{i=0}^{k-1} a_i\alpha^i$ en $b = \sum_{i=0}^{k-1} b_i\beta^i$. We volgen eerst de rekenregels van de formele machtreeksen:

$$\begin{aligned} ab &= (\textstyle\sum_{i=0}^{k-1} a_i\alpha^i)(\sum_{i=0}^{k-1} b_i\beta^i) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)\alpha + (a_0b_2 + a_1b_1 + a_2b_0)\alpha^2 + \ldots + (a_{k-1}b_{k-1})\alpha^{2k-2} \end{aligned}$$

We stellen hier echter vast dat er machten van α te voorschijn komen, die niet voorkomen in de vooropgestelde vorm van een element uit onze verzameling. We willen immers dat de hoogst voorkomende exponent bij α gelijk is aan $k-1$. We weten echter dat α een wortel is van een welbepaalde veelterm van graad k, dus $\alpha^k + c_1\alpha^{k-1} + c_2\alpha^{k-2} + \ldots + c_k = 0$ (met $x^k + c_1x^{k-1} + c_2x^{k-2} + \ldots + c_k$ een veelterm zonder oplossing in $\mathbb{Z}/_{p\mathbb{Z}}$). Dus vervangen we α^k door $-c_1\alpha^{k-1} - c_2\alpha^{k-2} - \ldots - c_k$, tot elke $\alpha^k, \alpha^{k+1}, \ldots$ vervangen werd door kleinere machten van α.

Voortbrengende veelterm Merk op, nu heb je optelling en vermenigvuldiging goed gedefinieerd, maar om aan te tonen dat deze bewerkingen samen met onze verzameling ook een *veld* uitmaken, is er nog een extra voorwaarde nodig. Elke bewerking op de coëfficiënten a_i voeren we uit in $\mathbb{Z}/_{p\mathbb{Z}}$, wat neerkomt op *modulo p* rekenen. Omdat p priem is, weten we dat eigenschap (5') (zie bijlage D: elk element heeft een multiplicatief invers) geldt in $\mathbb{Z}/_{p\mathbb{Z}}$: $\mathbb{Z}/_{p\mathbb{Z}}$ is dus een veld, terwijl $\mathbb{Z}/_{n\mathbb{Z}}$ (n niet priem) dat niet is. Elke bewerking op de elementen van onze nieuwe verzameling voeren we nu ook uit modulo $\alpha^k + c_1\alpha^{k-1} + \ldots + c_k$. Willen we dat eigenschap (5') ook geldt in onze nieuwe verzameling, dan moeten we een gelijkaardige voorwaarde opleggen aan die veelterm $\alpha^k + c_1\alpha^{k-1} + \ldots + c_k$ als aan p: de veelterm moet '*priem*' zijn, of in termen van veeltermen gesproken: onontbindbaar. (Dit is nog strenger dan '*geen oplossing hebben*'! Leg uit.) Deze veelterm noemen we de **voortbrengende veelterm** van ons veld van p^k elementen, en noteren we in wat volgt als $h(x)$.

Naamgeving Nu wordt het ook dringend tijd om onze nieuwe verzameling een naam te geven. Zouden we – via een totaal andere constructie – een andere verzameling van p^k elementen gevonden hebben, met andere notaties en andere definities van $+$ en $\times$, dan zullen we een één op één-relatie tussen de p^k elementen van beide verzamelingen kunnen vinden, waarbij bovendien de uitkomsten van de bewerkingen $+$ en $\times$ overeenkomen. Er bestaat dus in se maar één veld van de orde p^k. De theorie van de eindige velden werd ontwikkeld door Evariste Galois (1811-1832), vandaar de benaming voor een eindig veld van de orde p^k:

Definitie Het eindig veld van de orde p^k noteren we als $\mathbf{GF}(p^k)$, en noemen we **het Galoisveld** (Galois Field) van de orde p^k.

7.2 Rekenen in eindige velden

7.2.1 Veeltermen over $\mathbb{Z}/_{p\mathbb{Z}} = \mathbf{GF}(p^1)$

Vóór we het veld van p^k elementen verder bestuderen, moeten we gewoon worden aan rekenen met polynomen (eindige machtreeksen) over eindige verzamelingen (al dan niet een veld). Daarom volgende oefeningen.

Oefening 1

Werk uit in $\mathbb{Z}/_{3\mathbb{Z}}$: $(x+2)(x^2+2x+1)$.

Oefening 2

Werk uit in $\mathbb{Z}/_{n\mathbb{Z}}$*, zoals aangegeven (noteer enkel het resultaat, kladberekeningen doe je elders). Merk op:* $\mathbb{Z}/_{4\mathbb{Z}}$ *is geen veld.*

	$\mathbb{Z}/_{2\mathbb{Z}}$	$\mathbb{Z}/_{3\mathbb{Z}}$	$\mathbb{Z}/_{4\mathbb{Z}}$	$\mathbb{Z}/_{5\mathbb{Z}}$
$(x+1)^2$				
$(x+1)^3$				
$(x+1)^4$				
$(x+1)^5$				

Oefening 3

Werk uit in $\mathbb{Z}/_{n\mathbb{Z}}$*, zoals aangegeven (noteer enkel het resultaat, kladberekeningen doe je elders).*

	$n=3$	$n=5$	$n=7$
$(x+1)^n$			
$(x+2)^n$			
$(x+3)^n$			
$(x+4)^n$			
$(x+5)^n$			
$(x+6)^n$			

Oefening 4

Werk uit in $\mathbb{Z}/_{3\mathbb{Z}}$: $\dfrac{(x^3+x^2+x+1)}{(x+2)}$.

Let op! Bij een staartdeling voor veeltermen moet je regelmatig twee veeltermen van elkaar aftrekken. Dit wil wel eens mislopen; vooral als je ook aan modulorekenen moet denken. In dat geval kan je uiteraard teruggrijpen naar de techniek van de gelijkstelling van coëfficiënten. Omdat de graad van de teller 3 is, en de graad van de noemer 1, is de graad van de oplossing 2. Stel de oplossing gelijk aan $a_2x^2 + a_1x + a_0$, dan bekomen we de waarden van a_2, a_1 en a_0 uit de gelijkheid $(x^3 + x^2 + x + 1) = (x + 2)(a_2x^2 + a_1x + a_0) + r_0$. We houden hier rekening met een eventuele rest, wiens graad strikt kleiner is dan de graad van de deler (in dit geval: $0 < 1$).

Oefening 5

Wat is de rest van $f(x)$ bij deling door $(x + 1)$ respectievelijk $(x + 2)$? Beantwoord deze vraag voor $f(x) = x^4 + x^3 + x^2 + 1$ over $\mathbb{Z}/_{2\mathbb{Z}}$, $\mathbb{Z}/_{3\mathbb{Z}}$ en $\mathbb{Z}/_{5\mathbb{Z}}$.
Bevat de functie $f(x) = x^4 + x^3 + x^2 + 1$ een factor $(x + 1)$? Geef antwoord voor $\mathbb{Z}/_{2\mathbb{Z}}$, $\mathbb{Z}/_{3\mathbb{Z}}$ en $\mathbb{Z}/_{5\mathbb{Z}}$. (Doe zo min mogelijk rekenwerk!)

7.2.2 Ontbinden in factoren in het veld $\mathbb{Z}/_{p\mathbb{Z}} = \mathbf{GF}(p^1)$

Als we een veld $\mathbf{GF}(p^k)$, $k > 1$ willen construeren, dienen we een veelterm van graad k te vinden over $\mathbb{Z}/_{p\mathbb{Z}}$ die irreduciebel is. Met andere woorden: we moeten kunnen ontbinden in factoren over $\mathbb{Z}/_{p\mathbb{Z}}$ (of op z'n minst kunnen aantonen dat een ontbinding niet mogelijk is).

Gegeven een polynoom $f(x)$ van graad k over $\mathbb{Z}/_{p\mathbb{Z}}$. Om deze veelterm zo ver mogelijk te ontbinden in factoren, nemen we volgende stappen.

1. Eerst worden alle mogelijke lineaire factoren afgezonderd: $(x - a) \mid f(x) \Leftrightarrow f(a) = 0$. Omdat $\mathbb{Z}/_{p\mathbb{Z}}$ eindig is, kunnen we alle waarden voor a aflopen. Elke lineaire factor wordt uitgedeeld door middel van het algoritme van Horner (let vooral op meervoudige nulpunten!). De quotiëntveelterm die overblijft noemen we $f_1(x)$.[1]

2. Kan $f_1(x)$ nog verder ontbonden worden, dan zal elke factor in de ontbinding een veelterm van graad 2 of hoger zijn. We stellen een mogelijke ontbinding voorop (met voorlopig onbepaalde coëfficiënten), en passen de methode van gelijkstelling van coëfficiënten toe. Leidt het bekomen stelsel tot een tegenstrijdigheid, dan is $f_1(x)$ niet te ontbinden in factoren – of alleszins niet volgens de vooropgestelde verdeling.

[1] Toen je de regel van Horner destijds aanleerde, werd je waarschijnlijk verteld om enkel de delers van de constante term te controleren. (Weet je nog welke redenering hier achter stak?) In $\mathbb{Z}/_{p\mathbb{Z}}$ echter is elk getal deler van elk ander getal, dus controle van *alle* getallen uit $\mathbb{Z}/_{p\mathbb{Z}}$ blijft nodig!

Voorbeeld

Ontbind $f(x) = x^6 + x^3 + x + 1$ over $\boldsymbol{Z}/_{3\boldsymbol{Z}}$.

1. Eerst gaan we na of $f(x)$ lineaire factoren bevat. We rekenen uit: $f(0)$, $f(1)$ en $f(-1)$. (Merk op: machten van -1 zijn makkelijker te berekenen dan die van 2, dus gebruiken we $\{0, 1, -1\}$ als voorstelling voor $\boldsymbol{Z}/_{3\boldsymbol{Z}}$.) Gezien $f(0) \neq 0$, $f(1) \neq 0$ en $f(-1) = 0$ is -1 het enige mogelijke nulpunt. Met de methode van Horner gaan we na of dit nulpunt enkelvoudig is of niet.

	1	0	0	1	0	1	1
-1		-1	1	-1	0	0	-1
	1	-1	1	0	0	1	0
-1		-1	-1	0	0	0	
	1	1	0	0	0	1	

We zien dat $f(x) = (x+1)(x^5 - x^4 + x^3 + 1)$, maar dat de laatste factor (genaamd $f_1(x)$) geen nulpunten meer heeft. En dus ook geen lineaire factoren meer.

2. Daarom is de enige mogelijke opsplitsing van de graad van $f_1(x)$ gelijk aan $5 = 2 + 3$. We stellen een veelterm van de 2^e en een veelterm van de 3^e graad met nog onbepaalde coëfficiënten voorop:

$$(a_2x^2 + a_1x + a_0)(b_3x^3 + b_2x^2 + b_1x + b_0)$$

Omdat de coëfficiënt van x^5 gelijk is aan 1, mogen we $a_2 = b_3 = 1$ kiezen (de veeltermfactoren zijn op een constante na bepaald). We krijgen dus

$$\begin{aligned} h_1(x) &= x^5 - x^4 + x^3 + 1 \\ &= (x^2 + a_1x + a_0)(x^3 + b_2x^2 + b_1x + b_0) \\ \Leftrightarrow & \begin{cases} 1 = 1 & (5) \\ -1 = b_2 + a_1 & (4) \\ 1 = b_1 + a_1b_2 + a_0 & (3) \\ 0 = b_0 + a_1b_1 + a_0b_2 & (2) \\ 0 = a_1b_0 + a_0b_1 & (1) \\ 1 = a_0b_0 & (0) \end{cases} \end{aligned}$$

Uit (0) halen we twee mogelijkheden: ofwel is $a_0 = b_0 = -1$ ofwel is $a_0 = b_0 = 1$.

Eerste geval: $a_0 = b_0 = -1$.
Dan wordt het stelsel

$$\begin{cases} 1 = 1 \\ -1 = b_2 + a_1 \\ 1 = b_1 + a_1b_2 - 1 \\ 0 = -1 + a_1b_1 - b_2 \\ 0 = -a_1 - b_1 \\ 1 = a_0b_0 \end{cases}$$

De eerste en laatste gelijkheid zijn al voldaan. Werken we verder met de voorlaatste, dan onderscheiden we weer drie gevallen.

stel $a_1 = b_1 = 0$	stel $a_1 = 1 = -b_1$	stel $a_1 = -1 = -b_1$
$\begin{cases} 1 = 1 \\ -1 = b_2 \\ 1 = -1 \\ \quad ... \end{cases}$	$\begin{cases} 1 = 1 \\ -1 = b_2 + 1 \\ 1 = -1 + b_2 - 1 \\ \quad ... \end{cases}$	$\begin{cases} 1 = 1 \\ -1 = b_2 - 1 \\ 1 = 1 - b_2 - 1 \\ 0 = -1 - 1 - b_2 \\ \quad ... \end{cases}$

In elk van deze gevallen leidt $a_0 = b_0 = -1$ tot een tegenstrijdigheid.

Tweede geval: $a_0 = b_0 = 1$
Dan wordt het stelsel

$$\begin{cases} 1 = 1 \\ -1 = b_2 + a_1 \\ 1 = b_1 + a_1 b_2 + 1 \\ 0 = 1 + a_1 b_1 + b_2 \\ 0 = a_1 + b_1 \\ 1 = a_0 b_0 \end{cases}$$

Uit de voorlaatste gelijkheid halen we volgende gevallen:

stel $a_1 = b_1 = 0$	stel $a_1 = 1 = -b_1$	stel $a_1 = -1 = -b_1$
$\begin{cases} 1 = 1 \\ -1 = b_2 \\ 1 = 1 \\ 0 = 1 + b_2 \\ 0 = 0 + 0 \\ 1 = a_0 b_0 \end{cases}$ $\Leftrightarrow \begin{cases} a_0 = 1 \\ a_1 = 0 \\ b_0 = 1 \\ b_1 = 0 \\ b_2 = -1 \end{cases}$ $\Rightarrow$ ontbinding van $f_1(x)$ is $(x^2+1)(x^3-x^2+1)$	$\begin{cases} 1 = 1 \\ -1 = b_2 + 1 \\ 1 = -1 + b_2 + 1 \\ 0 = 1 - 1 + b_2 \\ \quad ... \end{cases}$ strijdigheid	$\begin{cases} 1 = 1 \\ -1 = b_2 - 1 \\ 1 = 1 - b_2 + 1 \\ \quad ... \end{cases}$ strijdigheid

... en UITERAARD reken je de oplossing na: $f(x) \stackrel{?}{=} (x+1)(x^2+1)(x^3-x^2+1)$.

Oefening 6

Welke veeltermen zijn reduciebel over $\mathbb{Z}/_{2\mathbb{Z}}$*?*

1. $f(x) = 1 + x + x^3 + x^4$
2. $f(x) = 1 + x + x^2$
3. $f(x) = 1 + x + x^2 + x^3$

4. $f(x) = 1 + x^4$
5. $f(x) = 1 + x + x^2 + x^3 + x^4$
6. $f(x) = 1 + x^2 + x^4$
7. $f(x) = 1 + x + x^3$
8. $f(x) = 1 + x^2 + x^3$

7.3 Notatie van de elementen van het eindig veld $\mathbf{GF}(p^k)$

Zoals vermeld is er slechts één veld van de orde p^k, voor gegeven priemgetal p en exponent k. Er zijn echter verschillende manieren om de p^k elementen van dit veld te noteren.

We zagen al dat de elementen genoteerd kunnen worden als veeltermen van maximale graad $k-1$ met coëfficiënten in het veld $\mathbb{Z}/_{p\mathbb{Z}}$, waarbij de 'onbekende' α in de veelterm opgevat kan worden als een symbool (net zoals het symbool i in $\mathbb{C}$). (We gebruiken het symbool α en niet x, zodat x nog gebruikt kan worden om vergelijkingen over $\mathbb{Z}/_{p\mathbb{Z}}$ op te lossen.)

Hadden we ook andere keuzes kunnen maken? Zouden we de elementen van bijvoorbeeld $\mathbf{GF}(4)$ ook eenvoudiger kunnen benoemen? Uiteraard. We zouden de namen a_0, a_1, a_2 en a_3 kunnen kiezen. We komen dan echter op een ander punt in de problemen: zodra we bewerkingen in $\mathbf{GF}(4) = \{a_0, a_1, a_2, a_3\}$ willen uitvoeren $(+, \times)$, zullen we ons moeten beroepen op de definitie van $+$ en $\times$ in dit veld: we zullen de optellings- en vermenigvuldigingstabel moeten kennen. Elke berekening impliceert dan uiteraard opzoekingswerk in de tabellen: plaats- en tijdrovend.

We zouden ook kunnen kiezen voor de notatie $\mathbf{GF}(4) = \{0, 1, 2, 3\}$. Opnieuw moeten we ons dan beroepen op de optellings- en vermenigvuldigingstabellen om bewerkingen op te zoeken. Laten we α met 2 overeenkomen en $\alpha + 1$ met 3, dan komt er (zie ook oef blz 108):

$\mathbf{GF}(4), +$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Dit is echter tegennatuurlijk: de optelling van de symbolen 1 en 3 resulteert dan in het symbool 2. Dit heeft niets meer vandoen met de fysische optelling van 2 aantallen (zoals 2+3=5 staat voor "2 appels en dan nog eens 3 appels geeft samen 5 appels"). Het is echter perfect mógelijk, als we ons niet verliezen in het vreemde hergebruik van symbolen.

Een derde mogelijkheid: we zouden de symbolen $\{0, 1, 2, 3\}$ kunnen vervangen door hun binaire voorstelling $\{(00), (01), (10), (11)\}$. Dit klinkt nu nog uit de lucht gegrepen, maar zal op blz 111 van nut blijken én dichter bij reële toepassingen liggen dan de notatie $\{0, 1, 2, 3\}$.

Laat ons echter voorlopig bij de notatie $\mathbf{GF}(4) = \{0, 1, \alpha, 1 + \alpha\}$ blijven. Voordeel hiervan: optellen is zeer eenvoudig (overeenkomstige termen van de veeltermen in α optellen, en

coëfficiënten in $\boldsymbol{Z}/_{p\boldsymbol{Z}}$ berekenen). Vermenigvuldigen gaat zoals bij gewone veeltermen, maar telkens er een term opduikt in α^k (of hoger), wordt α^k vervangen door $\alpha^k - h(\alpha)$, met $h(x)$ de onontbindbare veelterm die je uitkoos om de bewerkingen in $\mathbf{GF}(p^k)$ vast te leggen (zie oefening op blz 110). We hebben dus geen optellings- en vermenigvuldigingstabellen meer nodig (al is die soms wel handig als je berekeningen op papier maakt).

Oefening 7

We gebruiken in deze oefening(en) de veeltermnotatie voor de elementen van het Galoisveld van even orde. Geef de exacte orde van het Galoisveld, en som alle elementen van dit veld op, als je weet dat de voortbrengende functie $h(x)$ gegeven wordt door:

1. $h(x) = 1 + x + x^2$
2. $h(x) = 1 + x + x^3$
3. $h(x) = 1 + x^2 + x^3$

Oefening 8

Vul beide vermenigvuldigingstabellen aan: de eerste voor $\boldsymbol{Z}/_{4\boldsymbol{Z}}$, de tweede voor $\mathbf{GF}(4)$ met genererende functie $h(x) = 1 + x + x^2$.

$\boldsymbol{Z}/_{4\boldsymbol{Z}}, \times$	0	1	2	3
0				
1				
2				
3				

$\mathbf{GF}(4), \times$	0	1	α	$1+\alpha$
0				
1				
α				
$1+\alpha$				

Waar kan je uit afleiden dat de eerste dan wel de tweede verzameling een veld vormt met de bewerkingen $+$ en $\times$? Probeer daarna de laatste tabel te hermaken met genererende functie $h(x) = x + x^2$. Wat zie je?

Oefening 9

Voor je begint: noteer geen tussenresultaten in het schema, en laat boven en onder elke oplossing nog plaats (zie blz 111).
Vul de optellings- en vermenigvuldigingstabel aan voor het veld met genererende functie $h(x) = 1 + x + x^3$ *(coëfficiënten over* $\boldsymbol{Z}/_{2\boldsymbol{Z}}$*). Hoe kan je (zonder naar onderstaande tabellen te kijken) weten uit hoeveel elementen dit veld bestaat?*

$+$	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0								
1								
α								
$1+\alpha$								
α^2								
$1+\alpha^2$								
$\alpha+\alpha^2$								
$1+\alpha+\alpha^2$								

$\times$	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0								
1								
α								
$1+\alpha$								
α^2								
$1+\alpha^2$								
$\alpha+\alpha^2$								
$1+\alpha+\alpha^2$								

Oefening 10

Vul de optellings- en vermenigvuldigingstabel aan voor het veld met genererende functie $h(x) = 1 + x^2 + x^3$*, coëfficiënten over* $\boldsymbol{Z}/_2\boldsymbol{Z}$*. (Om vergelijking met oefening 7.3 te vereenvoudigen, kiezen we* β *als* 'imaginaire eenheid'*.)*

$+$	0	1	$1+\beta$	β	$1+\beta^2$	β^2	$\beta+\beta^2$	$1+\beta+\beta^2$
0								
1								
$1+\beta$								
β								
$1+\beta^2$								
β^2								
$\beta+\beta^2$								
$1+\beta+\beta^2$								

$\times$	0	1	$1+\beta$	β	$1+\beta^2$	β^2	$\beta+\beta^2$	$1+\beta+\beta^2$
0								
1								
$1+\beta$								
β								
$1+\beta^2$								
β^2								
$\beta+\beta^2$								
$1+\beta+\beta^2$								

Vergelijk het antwoord op de laatste twee oefeningen. Geef beide verzamelingen een duidelijker naam. Op het einde van volgende paragraaf zien we hoe de 8 elementen van deze verzameling(en) in bits voorgesteld (en bewerkt!) worden.

7.4 Toepassing in cryptografie

We hebben nu eindige velden geconstrueerd waarvan de kardinaliteit gelijk is aan een priemmacht. Kunnen we de typische veldeigenschap (nl. er bestaat altijd een multiplicatief invers) nu ook effectief gebruiken in informaticatoepassingen?

Stel dat we een bestand willen encrypteren. Dit hoeven we zelfs niet te onderstellen: zowat alle bitsgewijze informatie wordt geëncrypteerd. Is het niet om identiteit van zender / ontvanger en inhoud van de boodschap te beveiligen of om bestanden minder zwaar te maken, dan gebeurt het wel om extra controlemechanismen toe te voegen zodat storingen bij verzending opgevangen kunnen worden.

Elk encryptie-algoritme bestaat uit het omzetten van reeksen bits naar andere reeksen bits; telkens te interpreteren als gehele getallen. Deze omzettingen worden veelal gedefinieerd aan de hand van de bewerkingen $+$, $-$, $\times$, en... deling. Van zodra er een deling aan te pas komt, moeten we dus werken met bewerkingen in een veld. Anderzijds werken we best met gehele getallen die netjes passen binnen een gegeven aantal bits. Stel dat we data willen omzetten door telkens 8 bits tegelijk te bewerken. Met 8 bits kunnen we de getallen 0 tot en met 255 voorstellen. Maar $\boldsymbol{Z}/_{256\boldsymbol{Z}}$ is geen veld, dus deling is niet altijd mogelijk. Gebruiken we berekeningen in het veld $\boldsymbol{Z}/_{251\boldsymbol{Z}}$ (dichtste priemgetal), dan worden niet alle bitpatronen gebruikt, wat neerkomt op inefficiënt gebruik van geheugenruimte.

Maar zelfs als we een encryptie-algoritme opbouwen met enkel $+$, $-$, en $\times$ komen we met een verzameling die geen veld is in de problemen. Beschouw de vermenigvuldigingstabel van $\boldsymbol{Z}/_{8\boldsymbol{Z}}$ (blz 9). Daar zien we dat er meer kans zal zijn om een 4 tegen te komen in de uitkomst, dan een oneven getal. De vermenigvuldigingstabel van het veld $\mathbf{GF}(2^3)$ heeft dit onevenwicht niet, en is daarom geschikter voor codering van gegevens.

7.4.1 Coderen aan de hand van $\mathbf{GF}(2^k)$

Herneem de optellings- en vermenigvuldigingstabel van blz 109. We noteren de acht elementen van $\mathbf{GF}(2^3) = \mathbf{GF}(8)$ nu in de vorm van 3-bitswoorden. De coëfficiënt van α^2 staat vooraan. Vul bovenaan in elk kader de bitsgewijze representatie in; daaronder in potlood de decimale notatie (0-7).

- Wat merk je op voor de optelling? Welke operatie op bits heb je telkens doorgevoerd?
- Voor de vermenigvuldiging is een bitsgewijze operatie niet zo snel af te leiden. Laten we eerst nagaan wat een vermenigvuldiging met α (of bitpatroon (0 1 0)) betekent. Het element $a_2\alpha^2 + a_1\alpha + a_0$ (bitpatroon $(a_2\ a_1\ a_0)$) vermenigvuldigen met α levert $a_2\alpha^3 + a_1\alpha^2 + a_0\alpha$ op. De laatste 2 termen, $a_1\alpha^2 + a_0\alpha$, komen overeen met bitpatroon $(a_1\ a_0\ 0)$. Dit is de left shift over 1 bit toegepast op het oorspronkelijke patroon. De eerste term, $a_2\alpha^3$, vervangen we door $a_2(\alpha + 1)$ (want $h(x) = x^3 + x + 1$). Dit komt overeen met a_2 keer het bitpatroon (0 1 1). In woorden: een gegeven bitpatroon vermenigvuldigen met bitpatroon (0 1 0) komt neer op een left shift over 1 bit, met een

voorwaardelijke bitsgewijze XOR operator met (0 1 1) (nl. enkel indien het eerste bit van het gegeven bitpatroon 1 is).

Vermenigvuldiging met andere bitpatronen ((1 0 0), (1 1 0), (0 1 1), ...) wordt afgeleid uit de vermenigvuldiging met (0 1 0). Inderdaad:

$$\begin{array}{lll} (1\ 0\ 0) & \text{is gelijk aan} & (0\ 1\ 0) \times (0\ 1\ 0) \\ (1\ 1\ 0) & \text{is gelijk aan} & (1\ 0\ 0) + (0\ 1\ 0) \\ (0\ 1\ 1) & \text{is gelijk aan} & (0\ 1\ 0) + (0\ 0\ 1) \text{ enz.} \end{array}$$

Voorbeeld

Werk uit via bitoperaties; gebruik $h(x) = x^3 + x + 1$ als genererende functie van $\mathbf{GF}(2^3)$.

$$(0\ 1\ 1) \times (1\ 1\ 0) = \ldots$$

We schrijven eerst alle resultaten uit van vermenigvuldiging met machten van x.

$$\begin{array}{lllllll} (0\ 1\ 1) \times (0\ 1\ 0) & = & (1\ 1\ 0) & & & & \\ (0\ 1\ 1) \times (1\ 0\ 0) & = & (1\ 1\ 0) \times (0\ 1\ 0) & = & (1\ 0\ 0) + (0\ 1\ 1) & = & (1\ 1\ 1) \end{array}$$

Samenge(s)teld geeft dit:

$$\begin{array}{lll} (0\ 1\ 1) \times (1\ 1\ 0) & = & (0\ 1\ 1) \times (1\ 0\ 0) \ + \ (0\ 1\ 1) \times (0\ 1\ 0) \\ & = & (1\ 1\ 0) + (1\ 1\ 1) \\ & = & (0\ 0\ 1) \end{array}$$

Controle: $(x+1)(x^2+x) = x^3 + x^2 + x^2 + x = x^3 + x = x + 1 + x = 1$.

Oefening 11

Herneem bovenstaand voorbeeld voor een algemeen bitpatroon in plaats van het specifieke (0 1 1)*: bereken* $(a\ b\ c) \times (1\ 1\ 0)$.

Oefening 12

Gegeven is volgende codering van een 6-bitpatroon:

$$(a\ \ b\ \ c\ ;\ d\ \ e\ \ f) \rightarrow (a{+}b{+}c \quad d \quad b{+}c{+}e\ ;\ a{+}b{+}d{+}f \quad a{+}e \quad a{+}b{+}f)$$

Het patroon $(a\ \ b\ \ c\ ;\ d\ \ e\ \ f)$ *werd namelijk vermenigvuldigd met (0 0 0 ; 1 0 1), waarbij vermenigvuldiging met (0 0 0 ; 0 1 0) als volgt gedefinieerd wordt:*

$$(a\ \ b\ \ c\ ;\ d\ \ e\ \ f) \overset{\times(000;010)}{\rightarrow} (b\ \ c\ \ d\ ;\ e\ \ f\ \ 0) + a(1\ 1\ 1\ ;\ 1\ 0\ 1)$$

1. *Ga eerst na of* $(a\ \ b\ \ c\ ;\ d\ \ e\ \ f) \times$*(0 0 0 ; 1 0 1) inderdaad het gegeven bitpatroon oplevert.*
2. *Kan je (programmatorisch) nagaan of alle* 2^6 *bitpatronen in verschillende bitpatronen resulteren?*
3. *Wat is er mis met deze poging om de theorie van de eindige velden toe te passen om tot een 6-bitcodering te komen?*

Oefening 13

De Advanced Encryption Standard (AES) gebruikt berekeningen in het eindige veld $\mathbf{GF}(2^8)$*, met irreduciebele veelterm*

$$h(x) = x^8 + x^4 + x^3 + x + 1.$$

Bereken nu $(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1)$
en $(x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1)$ *op twee manieren: via polynomen en via bitsgewijze operatoren. (Voor het product via bitsgewijze operatoren bereken je dus eerst het product met alle machten van* x*!)*

Hoofdstuk 8

Grafentheorie: summiere inleiding

8.1 Definitie van grafen

Een graaf is een structuur van punten en verbindende lijnen. Denken we aan:

- een schematische weergave van het spoorwegennet (punten zijn stations, lijnen zijn spoorverbindingen)
- een stamboom (punten zijn mensen, lijnen duiden ouder-kindrelatie aan)
- de (gerichte) graaf van deelverzamelingen van een verzameling (punten zijn deelverzamelingen, lijnen duiden de inclusie-relatie aan en zijn dus gericht)

Meer formeel:

Definitie. *Een graaf G bestaat uit een eindige verzameling P, waarvan de elementen punten heten, en een verzameling E bestaande uit deelverzamelingen van P met twee punten. De elementen van E worden lijnen genoemd.*

Een graaf is een typisch discrete structuur: de punten zijn duidelijk van elkaar onderscheiden. Er komen wel lijnen in voor, maar een lijn moeten we als één object beschouwen, een plek ergens op een lijn heeft geen betekenis. Een lijn geeft enkel een relatie aan tussen de punten die zij verbindt. We introduceren een aantal begrippen uit de grafentheorie, zodat we een woordenschat hebben om elementaire graaftheoretische problemen te formuleren.

De punten van een graaf worden ook wel **toppen** of **knopen** genoemd (Engels: vertices). De lijnen van een graaf worden ook aangeduid met de termen **bogen** of **verbindingen** (Engels: edges).

Twee punten u en v die door een lijn verbonden zijn noemen we elkaars **buren**; de lijn of boog zelf noemen we uv. Worden de punten gelabeld met nummers of namen in plaats van

letters, dan noteren we de lijn door i en j als de verbinding (i, j). De punten u en v noemen we **incident** met de lijn uv, of: er bestaat een incidentie tussen u en uv. De punten u en v zelf noemen we dan **adjacent**.

Indien u en v gelijk zijn, is de verbinding een lus. Het is mogelijk dat tussen twee punten verschillende verbindingen bestaan. In dat geval spreekt met van **parallelle verbindingen** of multibogen. Indien dit voorkomt spreekt men van **multigrafen**. We zullen ons echter vooral om **enkelvoudige** grafen bekommeren: grafen zonder lussen en zonder parallelle verbindingen.

Verbindingen kunnen expliciet een richting aanduiden: dan spreekt men van een **gerichte** graaf. Een verbinding wordt dan aangeduid door zijn begin- en eindknoop, **in die volgorde**: verbinding (i, j) is dus niet dezelfde als verbinding (j, i). Bij een niet-gerichte graaf bestaat dat onderscheid niet: beide stellen dezelfde verbinding voor. Een knoop van een gerichte graaf kan ook met zichzelf verbonden worden (**selfloop**).

De graad $d(v)$ van een punt v van de graaf is het aantal buren dat hij heeft. Bij een gerichte graaf heeft elke knoop een **ingraad** en een **uitgraad**. De ingraad is het aantal knopen waarvan hij buur is (het aantal inkomende verbindingen), de uitgraad is het aantal buren van de knoop (het aantal uitgaande verbindingen).

Een graaf wordt **samenhangend** genoemd als er tussen elk paar toppen x, y een opeenvolging van adjacente toppen $x \sim z_1 \sim z_2 \sim \ldots \sim z_k \sim y$ bestaat. Dergelijke opeenvolging noemen we een **pad**. Een gesloten pad (i.e. begin- en eindtop zijn gelijk) noemen we een **cykel**. Is een graaf niet samenhangend, dan valt hij uiteen in samenhangende componenten. Elke component bestaat uit een deelverzameling van de toppenverzameling van de graaf, tesamen met alle bogen die incident zijn met deze toppen.

Een **boom** is een samenhangende ongerichte graaf, die geen selfloops of cykels heeft.

In de cursus *Algoritmen en Gegevensstructuren* (3e bachelor en master) worden bomen en grafen uitvoerig behandeld — vooral met het oog op efficiënte algoritmen op grafen. We beperken ons hier tot enkele wiskundige stellingen.

8.2 Voorstelling van grafen

Willen we grafen voorstellen, dan hebben we verschillende mogelijkheden.

1. Als de graaf niet groot is, kunnen we hem tekenen. Het zal echter niet altijd op zicht duidelijk zijn of twee tekeningen in se dezelfde graaf voorstellen.
2. Als de graaf groot en **dicht** is (i.e. aantal bogen is relatief groot ten opzichte van aantal toppen), dan kunnen we voor een adjacentiematrix opteren. Dit is een matrix waarbij rijen én kolommen voor toppen staan, en het matrixelement $a_{ij} \in \{0, 1\}$ aangeeft of top i al dan niet adjacent is met top j ($a_{ij} = 1 \Leftrightarrow i \sim j$). Voor een ongerichte graaf zal de helft van de matrix volstaan, gezien $a_{ij} = a_{ji}$.

3. Als de graaf groot en **ijl** (=niet dicht) is, zal zijn adjacentiematrix teveel nullen bevatten. Dus teveel geheugenruimte voor te weinig nuttige informatie. In programmeertoepassingen wordt dan geopteerd voor een burenlijst: elke top i houdt een lijstje bij van al zijn buren.

We geven een stelling die verband houdt met de grafische voorstelling van grafen en een inleiding op het vierkleurenprobleem voor vlakke grafen. Daarna enkele stellingen die verband houden met de adjacentiematrix van een graaf.

8.3 Vlakke grafen

Een (ongerichte) graaf is vlak wanneer zijn knopen zo in een vlak kunnen geplaatst worden dat zijn verbindingen niet snijden. (In dat geval kan men zelfs aantonen dat de knopen zo kunnen geplaatst worden dat alle verbindingen *rechte* lijnstukken zijn.) Nagaan of een graaf vlak is kan in lineaire tijd, gebaseerd op diepte-eerst[1] zoeken.

8.3.1 Eulerformule voor vlakke grafen

Een vlakke graaf verdeelt het vlak in een aantal gebieden (met inbegrip van het buitengebied). Er bestaat een belangrijk verband tussen het aantal knopen **k**, het aantal verbindingen V en het aantal gebieden **G** van een vlakke graaf bestaande uit c samenhangende componenten, gegeven door de formule van Euler: $\mathbf{k} - \mathrm{V} + \mathbf{G} = c + 1$. Deze formule geldt niet alleen voor enkelvoudige grafen, maar ook voor grafen die meerdere verbindingen tussen twee knopen toelaten (multigrafen), of lusverbindingen waarvan de begin- en eindknopen samenvallen (selfloops). Er bestaat ook een algemenere formule voor grafen in meer dimensies.

Stelling 8.1. *Voor een vlakke graaf bestaande uit c samenhangende componenten,* **k** *knopen, V verbindingen en* **G** *gebieden (buitengebied inbegrepen), geldt*

$$\mathbf{k} - V + \mathbf{G} = c + 1$$

Bewijs We tonen eerst aan dat de formule geldt voor een samenhangende graaf ($c = 1$). Deze formule moet gelden voor elke $\mathbf{k} \in \mathbb{N}$, elke $\mathrm{V} \in \mathbb{N}$, ... Dit wijst erop dat we een bewijs via inductie nodig hebben. Daarvoor moeten we eerst beslissen op welke variabele we inductie toepassen; het wordt hier V.[2]

BASIS Voor een samenhangende graaf met slechts één verbinding geldt de formule zeker. Ofwel heeft deze graaf twee knopen als eindpunten van de verbinding, ofwel één knoop met een lusverbinding. In het eerste geval is er slechts één gebied, in het tweede geval zijn er twee.

[1] Zie cursus *Algoritmen*, en Hopcroft en Tarjan, 1974.

[2] Hoe meer verbindingen je legt tussen een vast aantal knopen, hoe moeilijker het is om de graaf vlak te houden. Dit geeft aan dat **k** constant laten en V variabel maken, in de goede richting gaat.

STAP Onderstel dat de formule geldt voor elke samenhangende graaf met $\mathbf{k}$ toppen en met $\mathrm{V}-1$ verbindingen. Dan tonen we aan dat ze ook geldt voor een samenhangende graaf met $\mathbf{k}$ toppen en met V verbindingen. Dat is zeker zo als die graaf een boom is, want dan is $\mathrm{V}=\mathbf{k}-1$, en er is slechts één gebied. Als de graaf geen boom is, dan heeft hij minstens één lus (eventueel een lusverbinding). Als we een verbinding van die lus wegnemen, dan blijft de graaf samenhangend, en dus geldt de inductieveronderstelling. Deze nieuwe graaf heeft evenveel knopen als de oorspronkelijke, maar één verbinding en één gebied minder (de lus werd immers geopend). We krijgen dan:

$$\mathbf{k}-(\mathrm{V}-1)+(\mathbf{G}-1)=2$$

Uitgewerkt geeft dat het gezochte resultaat.

Een niet-samenhangende graaf bestaat uit c samenhangende componenten, en voor elke component i met $\mathbf{k}_i$ knopen, V_i verbindingen en $\mathbf{G}_i$ gebieden geldt dus de formule

$$\mathbf{k}_i-\mathrm{V}_i+\mathbf{G}_i=2$$

Tellen we al die formules lid-per-lid op, dan krijgen we

$$\sum_{i=1}^{c}\mathbf{k}_i-\sum_{i=1}^{c}\mathrm{V}_i+\sum_{i=1}^{c}\mathbf{G}_i=2c$$

Nu is $\sum_{i=1}^{c}\mathbf{G}_i=\mathbf{G}+c-1$, want het buitengebied werd $c-1$ maal teveel geteld. Dus komt er

$$\mathbf{k}-\mathrm{V}+\mathbf{G}+(c-1)=2c$$

en dat geeft uiteindelijk de gezochte algemene formule. □

8.3.2 Bovengrens voor aantal verbindingen in vlakke (enkelvoudige) grafen

Merk op dat het geen zin heeft om de grootheid $\mathbf{G}$ af te lezen van een niet-vlakke tekening van een vlakke graaf. Dan zijn de gebieden immers niet makkelijk te detecteren. Hoe kom je dan snel te weten of een relatief kleine, getekende graaf toch vlak is? Je kan immers uit de tekening enkel $\mathbf{k}$ en V afleiden, en mits een goed gekozen algoritme ook c. We onderstellen voorlopig dat de graaf samenhangend en enkelvoudig is (dus $c=1$ en geen multibogen). We elimineren nu $\mathbf{G}$ uit de formule van Euler, zodat enkel $\mathbf{k}$ en V overblijven. Om dit te doen, drukken we $\mathbf{G}$ uit in functie van V. Dit kan met een dubbele telling op het aantal verbindingen en het aantal gebieden. We tellen het aantal koppels (β,γ) waarbij β een verbinding is die deel uitmaakt van de grens van het gebied γ. Elk van de $\mathbf{G}$ gebieden heeft minstens 3 verbindingen in zijn grens. Elk van de V verbindingen ligt op de grens van hoogstens 2 verschillende gebieden. We krijgen dus $3\mathbf{G}\leq 3^{+}\mathbf{G}=2^{-}\mathrm{V}\leq 2\mathrm{V}$ of $3\mathbf{G}\leq 2\mathrm{V}$. (We noteerden 'minstens 3' met 3^{+}, en 'hoogstens 2' met 2^{-}.) Samen met de formule van Euler krijgen we dan

$$3\mathrm{V}-3\mathbf{k}+6\leq 2\mathrm{V}$$

zodat tenslotte

$$\mathrm{V} \leq 3\mathbf{k} - 6 \qquad (\text{voor } \mathbf{k} \geq 3)$$

Wanneer de graaf geen enkel driehoekig gebied bevat, geldt zelfs

$$4\mathbf{G} \leq 2\mathrm{V}$$

zodat nu

$$\mathrm{V} \leq 2\mathbf{k} - 4$$

Deze ongelijkheden gelden niet alleen voor een samenhangende graaf, want een niet-samenhangende graaf met evenveel knopen heeft minder verbindingen. Voor een enkelvoudige vlakke graaf is dus in elk geval het aantal verbindingen van dezelfde grootte-orde als het aantal toppen ($m = O(n)$). Deze grafen zijn dus ijl.

Deze ongelijkheden worden gebruikt om na te gaan of een graaf vlak is. Onderstaande kleine grafen zijn belangrijk voor de vlakheid van grotere grafen: als een grote graaf deelgrafen heeft van onderstaande vorm, is die grote graaf zeker niet vlak.

Voorbeeld

> Nemen we K_5, een complete graaf[3] met vijf knopen. Deze graaf heeft driehoekige gebieden, en met $\mathbf{k} = 5$ en $\mathrm{V} = 10$ is niet aan de eerste ongelijkheid voldaan, zodat K_5 niet vlak is.

Voorbeeld

> Als tweede voorbeeld nemen we de bipartiete graaf $K_{3,3}$ met zes knopen,[4] verdeeld in twee groepen van drie, waarbij elke knoop van de ene groep met elke knoop van de andere verbonden is. Deze graaf heeft geen driehoekige gebieden, en met $\mathbf{k} = 6$ en $\mathrm{V} = 9$ is niet aan de tweede ongelijkheid voldaan, zodat $K_{3,3}$ evenmin vlak is.

8.3.3 Vierkleurenprobleem

Een inkleuring van een graaf bestaat uit het inkleuren van de toppen, zodat adjacente toppen nooit dezelfde kleur hebben. Elke vlakke graaf (en dus elke landkaart, als je landen voorstelt door toppen en gemeenschappelijke grenzen door bogen), kan ingekleurd worden met vier kleuren. In 1976 vond men het bewijs van dit 'longstanding conjecture'[5]. Het bewijs is echter

[3] Een complete graaf heeft een verbinding tussen elk paar knopen. Ook wel 'clique' genoemd.

[4] De 'K' komt van de wiskundige Kuratowski, de eerste om vlakke grafen te karakteriseren.

[5] Een conjecture is een uitspraak waarvan iedereen (i.e. alle mensen die vertrouwd zijn met de materie) aanneemt, aanvoelt en/of vermoedt dat ze wel waar móet zijn (omdat er bvb. voldoende aanwijzingen zijn, of omdat de uitspraak meer dan goed aansluit bij de reeds gekende theorieën,...) maar waarvan totnogtoe niemand het formele bewijs heeft kunnen vinden. Een (voor)oordeel dat van weinig onderzoekszin getuigt zou dan zijn '*deze uitspaak kán gewoon niet waar zijn*', een betere tactiek is: erkennen dat er nog werk aan de winkel is (en misschien zelf op zoek gaan naar andere bewijsmethodes?). Het is onder wiskundigen trouwens een sport om bewijzen die geleverd werden door gebruik te maken van een conjecture, toch trachten te herdoen zonder conjecture: via een andere weg (meestal een omweg). Idem voor bewijzen waarvoor de computer ingeschakeld werd: dan is de jacht op een meetkundig bewijs open!

een uitgebreide gevallenstudie uitgevoerd met de computer. Dit valt dus buiten het bereik van deze cursus. Maar het bewijs dat vijf kleuren volstaan, kunnen we wel geven.

Stelling 8.2. *Elke vlakke graaf kan ingekleurd worden met vier (of minder) kleuren.*

Bewijs Buiten het bereik van deze cursus. □

Lemma 8.3. *Elke vlakke graaf kan ingekleurd worden met vijf (of minder) kleuren.*

Bewijs We wijzen erop dat het enkel nodig is om het bewijs te leveren voor een samenhangende graaf. Je voelt ook aan dat, hoe meer toppen (of landen) er zijn, hoe moeilijker de inkleuring wordt. Dit leidt ons naar de juiste bewijsmethode: bewijs via inductie op de toppen.

BASIS Als de graaf G 5 of minder toppen heeft, kunnen we uiteraard een graafkleuring vinden met 5 kleuren.

STAP

INDUCTIEHYPOTHESE

Stel dat elke vlakke graaf met $\mathbf{k}-1$ toppen kan gekleurd worden met 5 kleuren.

TE BEWIJZEN

We willen aantonen dat elke graaf met $\mathbf{k}$ toppen een 5-kleuring toelaat.

Beschouw een vlakke graaf G met $\mathbf{k}$ toppen. Elke deelgraaf van G die één top minder heeft (en dus ook een aantal verbindingen minder), voldoet aan de voorwaarde van de inductiehypothese. Zo zijn er $\mathbf{k}$ deelgrafen. Stel dat je een deelgraaf G$'$ koos, die je bekomt door een top τ weg te laten van graad 20. De deelgraaf G$'$ is gekleurd met 5 kleuren. Welke kleur moet top τ dan krijgen om G te kleuren? Er zullen 20 verbindingen gecontroleerd moeten worden — veel te veel. Moest de top τ slechts graad 1, 2, 3 of 4 hebben dan zou de 5-kleuring wél makkelijk zijn. Dus: kies een top τ die zo weinig mogelijk verbindingen heeft, en stel $\mathrm{G}' = \mathrm{G} \setminus \{\tau\}$. Wat is echter '*zo weinig mogelijk*' verbindingen? Is dit kleiner dan 5, of toch nog groter? Daartoe tellen we het aantal toppen van graad i ($i \in \mathbb{N}$); met de techniek van de dubbele telling. Stel dat $\mathbf{k}_i$ het aantal toppen is van graad i, en stel l de grootst mogelijke graad van een top. Het is duidelijk dat

$$\mathbf{k} = \mathbf{k}_1 + \mathbf{k}_2 + \mathbf{k}_3 + \ldots + \mathbf{k}_l.$$

Tellen we het aantal koppels (τ, β) waarbij top τ incident is met boog β, dan krijgen we

$$\left.\begin{array}{rcl} \mathbf{k}_1 + 2\mathbf{k}_2 + 3\mathbf{k}_3 + \ldots + l\mathbf{k}_l & = & 2\mathrm{V} \\ & \leq & 2(3\mathbf{k} - 6) \\ & = & 6\mathbf{k}_1 + 6\mathbf{k}_2 + \ldots + 6\mathbf{k}_l - 12 \end{array}\right| \text{ dubbele telling + Eulerformule}$$

Hieruit volgt:

$$12 \leq \mathbf{k}_7 + 2\mathbf{k}_8 + 3\mathbf{k}_9 + \ldots + (k-6)\mathbf{k}_l + 12 \leq 5\mathbf{k}_1 + 4\mathbf{k}_2 + 3\mathbf{k}_3 + 2\mathbf{k}_4 + \mathbf{k}_5.$$

Hieruit volgt dat er minstens één van de waarden $\mathbf{k}_i$ $(i = 1 \to 5)$ verschillend is van nul.

Nu kunnen we voort met onze redenering. We weten dat er (minstens) één top τ is van graad ≤ 5. We beschouwen de deelgraaf G$'$ door τ en diens verbindingen weg te laten uit G. Uit de inductiehypothese mogen we besluiten dat G$'$ kan ingekleurd worden met vijf kleuren. Werden er voor de inkleuring van de buren van τ (maximaal 5 in aantal) maximaal 4 kleuren gebruikt, dan is er nog een kleur over voor τ zelf. Daarmee is G gekleurd.

Werden er voor de inkleuring van de buren van τ vijf kleuren gebruikt, dan is τ dus van graad 5, en moeten we verder onderzoek uitvoeren. We zullen ook hier ons moeten baseren op het feit dat de graaf vlak is. We tekenen de 5 buren van τ, en nummeren de buren met de klok mee. Dit nummer slaat meteen ook op de gebruikte kleuren. Nu hebben de 5 buren een naam: $\tau_1, \tau_2, \ldots, \tau_5$. Wat we nodig hebben om τ een kleur te geven, is een kleurenswitch voor minstens één τ_i. Stel dat we vanuit top τ_i vertrekken, en alle paden aanduiden die enkel kleuren i en j (voor zekere j) bevatten. Deze structuur zal een tweekleurige deelgraaf vormen. Als deze deelgraaf geen enkele andere buur van τ bevat (deze buur zou dan noodgedwongen τ_j zijn, gezien de deelgraaf afwisselend kleuren i en j gebruikt), dan kunnen we alle toppen van deze deelgraaf van kleur switchen (i wordt j en omgekeerd), zonder conflicten op te roepen. We tonen dus aan dat we dergelijke deelgraaf vinden, met een bewijs uit het ongerijmde.
Stel dat we vanuit geen enkele buur van τ een dergelijke tweekleurige deelgraaf vinden. Met 'dergelijk' bedoelen we 'niet uitmondend in een andere buur van τ'. Dan moet dus de deelgraaf die in τ_1 vertrekt en uit kleuren 1 en 3 bestaat, ergens een tweekleurig pad π_{13} hebben dat in τ_3 aankomt. Analoog zal er een tweekleurig pad π_{24} vanuit τ_2 naar τ_4 bestaan. Gezien G$'$ vlak is, mogen de paden π_{13} en π_{24} elkaar niet kruisen, maar moeten ze een top gemeen hebben. (Zie schets: ligging van τ_2 tussen τ_1 en τ_3 is van belang, evenals ligging van τ_3 tussen τ_2 en τ_4.) Deze top zou tegelijkertijd kleur 1 of 3 én kleur 2 of 4 moeten hebben. Dit is een contradictie.
Gevolg: er bestaat een τ_i met een deelgraaf in de kleuren i en j, die niet uitmondt in de top τ_j (desnoods is deze deelgraaf leeg). Wisselen we alle toppen van deze deelgraaf van kleur, dan schiet er een kleur over om aan τ te geven. □

8.4 Incidentiematrices en afgeleide resultaten

Gebruiken we de matrixvoorstelling voor een graaf G, dan kunnen we bewerkingen op deze matrix linken met eigenschappen van de graaf. We denken hierbij aan bepaling van het aantal mogelijke paden tussen twee knopen, lengte van kortste pad tussen twee knopen, transitieve sluiting van een graaf. Afhankelijk van de gekozen bewerkingen op de incidentiematrix A van graaf G, vinden we het antwoord op één van deze problemen.

Merken we eerst op dat er voor een enkelvoudige graaf enkel nullen en enen in de incidentiematrix staan. Bij een multigraaf kunnen we het matrixelement a_{ij} gelijk stellen aan het *aantal* bogen (of pijlen) van i naar j. Dit geeft dus entries die groter kunnen zijn dan 1.

8.4.1 Betekenis van $A \times A$

Gegeven een graaf G met n knopen. Stellen we $A \times A = B = (b)_{ij}$, dan is b_{ij} gedefinieerd als $b_{ij} = \sum_{l=1}^{n} a_{il}a_{lj}$. Het element a_{il} geeft het aantal verbindingen tussen knoop i en l. Het element a_{lj} geeft het aantal verbindingen tussen knoop l en j. Het product $a_{il}a_{lj}$ geeft dus het aantal verbindingen tussen i en j via l. Merk op dat het productprincipe hier van toepassing is. Willen we het totale aantal verbindingen van lengte 2 tussen i en j kennen, onafhankelijk van de tussenknoop l, dan moeten we (gezien het somprincipe) alle producten $a_{il}a_{lj}$ sommeren. Met andere woorden: de matrix $A \times A$ is de matrix die voor elk koppel (i, j) het aantal paden van lengte 2 tussen knoop i en knoop j bijhoudt.

Tip Leer deze tekst niet van buiten, maar maak een schets waarop je de redenering volgt. Links knoop i, rechts knoop j, en daartussen verticaal onder elkaar alle knopen van 1 tot en met n.

8.4.2 Betekenis van $A^k = (a^{[k]})_{ij}$

Via inductie tonen we aan dat $a_{ij}^{[k]}$ gelijk is aan het aantal paden van lengte k tussen i en j. De basis ($k = 2$, zelfs $k = 0$ en $k = 1$) is in orde. We weten $A^k = A^{k-1} \times A$. Uit de inductiehypothese is $a_{il}^{[k-1]}$ het aantal paden van lengte $k - 1$ tussen knoop i en knoop l. Het element a_{lj} van A is het aantal verbindingen tussen l en j. Gecombineerd via het productprincipe, is $a_{il}^{[k-1]}a_{lj}$ dus het aantal paden tussen i en j, waarbij knoop l op de voorlaatste plaats van het pad staat. Gecombineerd via het somprincipe, is $\sum_{l=1}^{n} a_{il}^{[k-1]}a_{lj} = a_{ij}^{[k]}$ het aantal paden van lengte k tussen i en j.

Merk op: als we met een gerichte graaf te maken hebben waarbij (i, j) én (j, i) een pijl voorstellen, dan zal tussen i en j ook het pad $i \to j \to i \to j$ geteld worden als pad van lengte drie. Niet echt nuttig? Misschien is het voldoende ons af te vragen óf er een pad is tussen i en j. Zo komen we op de transitieve sluiting van een graaf.

8.4.3 Transitieve sluiting van een graaf

De **transitieve sluiting** van een **gerichte graaf** is de graaf die voor elk pad van x naar y, ook een rechtstreekse verbinding van x naar y heeft. Is er in de transitieve sluiting dus geen verbinding tussen x en y, dan is y niet bereikbaar vanuit x. Denk hierbij aan de boom die een partiële orderelatie weergeeft in een verzameling, bijvoorbeeld *is nakomeling van* in een stamboom. Om de tekening van een stamboom overzichtelijk te houden, duiden we alleen directe ouder-kind relaties aan. De transitieve sluiting geeft echter voor elk voorouder-nakomeling-koppel een verbinding.

Bepaling van de transitieve sluiting van een **ongerichte graaf** zal neerkomen op het bepalen van de samenhangende componenten. Teken je op elke samenhangende component de volledige graaf (d.i. de graaf waarbij elk paar knopen verbonden is), dan heb je de transitieve sluiting.

Voor de bepaling van de transitieve sluiting van een graaf, is het voldoende ons af te vragen óf er een pad is tussen i en j. Hierbij speelt het aantal paden en de lengte van het pad geen rol.

1. Beschouwen we eerst de paden tussen i en j van lengte 1. Die zijn te vinden in de matrix A. Gezien enkel het bestaan en niet het aantal ons interesseert, nemen we hiervoor de versie met enkel nullen en enen als entries.

2. Beschouwen we het bestaan van een pad van lengte 2 tussen i en j. We willen de informatie hiervan opslaan in de matrix $A \times A = A^{[2]}$ zoals hierboven — eventueel met lichte wijziging van berekeningsmethode.
   Gegeven een knoop l. Er gaat een pad van lengte 2 van i naar j over l als en slechts als $a_{il} = 1$ én $a_{lj} = 1$. Dus $a_{il}a_{lj} = 1$ als en slechts als dergelijk pad bestaat.
   Er bestaat een pad van lengte 2 tussen i en j, zodra er één l is waarvoor $a_{il}a_{lj} = 1$. Definiëren we $a_{ij}^{[2]}$ als het maximum van alle $a_{il}a_{lj}$, dan zal $A^{[2]}$ inderdaad de matrix zijn die het bestaan van paden van lengte 2 bijhoudt.

3. We moeten dus overgaan op een andere berekening van het matrixproduct: we starten met een matrix met enkel nullen en enen, vermenigvuldiging blijft vermenigvuldiging, maar de optelling wordt vervangen door het maximum.

4. Hoever moeten we nu doorgaan om de adjacentiematrix van de transitieve sluiting te vinden? In principe zou je alle $A^{[k]}$ moeten sommeren. Is echter $k = n + 1$ (met n het aantal knopen van de graaf), dan geeft $a_{ij}^{[n+1]}$ aan of er een pad van lengte $n + 1$ tussen i en j bestaat. Een pad van lengte $n + 1$ bevat n knopen tussen x en y. Gezien x gelijk zou kunnen zijn aan y, moeten die n knopen dus genomen worden uit $n - 1$ knopen ($\neq x, \neq y$) van de graaf. Dit impliceert dat één knoop minstens tweemaal voorkomt, stel op plaats δ en $\delta + \epsilon$. Laten we het deel van het pad tussen plaats δ en $\delta + \epsilon$ weg, dan hebben we dus een pad gevonden tussen i en j dat korter is dan $n + 1$. Met dit pad werd al rekening gehouden in de matrix $A^{[n+1-\epsilon]}$, dus brengt de matrix $A^{[n+1]}$ geen wezenlijke informatie meer aan. Analoog voor alle matrices $A^{[k]}$, $k \geq n + 1$.

Zo komen we op volgende stelling.

Stelling 8.4. *De adjacentiematrix van de transitieve sluiting van een graaf met n toppen is gedefinieerd als*

$$A + A^{[2]} + \ldots + A^{[n]}$$

waarbij optelling over $\{0, 1\}$ *gedefinieerd wordt als* **max** *(*$0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 1$*).*

Bewijs Zie voorafgaande redenering. □

8.4.4 Minimumafstand in gewogen grafen

Een **gewogen graaf** is een gerichte graaf, waarbij elke pijl een bepaald gewicht meekrijgt. Dit gewicht staat voor de 'lengte' of de 'kost' van de verbinding. (Denk bvb aan reistijden om van punt A naar punt B te raken, volgens een bepaalde weg.) We kunnen een gewogen gerichte graaf voorstellen door zijn gewichtenmatrix $A = (a)_{ij}$. Zijn twee punten niet verbonden, dan stellen we de kost in op ∞. De diagonaalelementen krijgen de waarde 0. De weg om van i via l naar j te raken, is dan de som van de gewichten a_{il} en a_{lj}. De kortste (of goedkoopste) weg om met één tussenstap van i naar j te geraken, is dan het minimum van alle gewichten $a_{il} + a_{lj}$, $l = 1 \to n$. Met deze alternatieve bewerkingen ($+$ in plaats van $\cdot$ en **min** in plaats van $+$), zal de matrix $A \times A = A^{[2]} = (a^{[2]})_{ij}$ de kortste weg geven van i naar j met één tussenstop.
Analoog zal $A^{[k]}$ de gewichtenmatrix zijn van de gerichte graaf die bestaat uit de paden van lengte k in de graaf G.

Willen we het pad vinden met het kleinste gewicht tussen i en j, dan berekenen we

$$\mathbf{min}(J, A, A^{[2]}, A^{[3]}, \ldots, A^{[n-1]}),$$

waarbij $J = \begin{pmatrix} 0 & \infty & \vdots & \infty \\ \infty & 0 & & \infty \\ \ldots & & \ddots & \infty \\ \infty & \infty & \infty & 0 \end{pmatrix}$ de gewichten van de paden van lengte 0 voorstelt. We moeten $A^{[n]}$ (en verder) niet meer beschouwen, omdat elk pad dat n of meer pijlen bevat, minstens één knoop tweemaal bevat. Laten we de cykel hiertussen weg, dan hebben we een korter pad, dat we al in rekening brachten in een vorige matrix.

Stelling 8.5. *De minimum lengte van een pad tussen i en j in een gerichte gewogen graaf met n knopen, is het element* c_{ij} *uit de matrix*

$$C = \mathbf{min}(J, A, A^2, \ldots, A^{n-1}).$$

Matrixvermenigvuldiging wordt hierbij gedefinieerd door $(A \times B)_{ij} = min(a_{i1} + b_{1j}, a_{i2} + b_{2j}, \ldots, a_{in} + b_{nj})$*, en J is de eenheidsmatrix voor de aldus gedefinieerde matrixvermenigvuldiging.*

Bewijs Zie voorafgaande redenering. □

Opmerking Zie je in waarom er nu tot $A^{[n-1]}$ gerekend wordt, terwijl er bij de transitieve sluiting tot $A^{[n]}$ doorgewerkt wordt? Dit heeft met cykels te maken: als begin- en eindpunt van het pad gelijk zijn aan elkaar. Als we stellen dat het gewicht van de lus (x, x) gelijk is aan nul, moeten we geen cykels meer beschouwen (nul is sowieso het minimumgewicht).

Oefening 1

Bereken de transitieve sluiting van de gerichte graaf met verbindingen

$$(1,5),(5,4),(4,3),(3,2),(3,1).$$

Doe dit zowel via de adjacentiematrix als via een schets.

Oefening 2

Bereken het aantal paden van lengte twee tussen knopen van de gerichte multigraaf met verbindingen

$$(1,2),(1,2),(2,3),(3,4),(2,4),(1,4),(4,4),(1,3).$$

Oefening 3

Toon aan dat de samenhangende componenten van een ongerichte graaf kunnen afgeleid worden uit een uitdrukking van de vorm $A + A^2 + \ldots + A^n$. Geef hierbij aan waar A voor staat, en hoe de machten van A berekend worden. Geef een klein voorbeeld op een graaf van 6 knopen, met 3 samenhangende componenten van ongelijke grootte.

Oefening 4

Bereken de kortste afstand tussen de vier knopen van de gewogen graaf G*, met verbindingen*

$$(1,2),(1,3),(1,4),(2,1),(2,3),(3,1),(3,4),(4,2)$$

en respectieve gewichten

$$1 \quad 3 \quad 3 \quad 2 \quad 2 \quad 4 \quad 2 \quad 3.$$

Opmerking

Het moge duidelijk zijn dat de hierboven aangehaalde stellingen niet bruikbaar zijn in informaticatoepassingen als het om ijle grafen gaat (inefficiënt geheugengebruik), en dat er ook voor dichte grafen veel efficiëntere algoritmen bestaan. Deze stellingen geven enkel de kracht van het (al dan niet licht gewijzigde) matrixrekenen aan. Ook via de eigenwaarden van de adjacentiematrix van een graaf kan men mooie resultaten bekomen.

Bijlage A

Faculteit

De bewerking '!' (lees: faculteit) op een natuurlijk getal $n \in \mathbb{N}$ wordt als volgt gedefinieerd:

$$n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$$

We definiëren voorts voor $k \leq n$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Oefening 2

Bereken:

1. $7! =$
2. $\dfrac{10!}{8!} =$
3. $\dfrac{10!}{4!6!} =$

Oefening 3

Toon volgende gelijkheden aan

1. $\binom{n}{k} = \binom{n}{n-k}$
2. $\binom{n}{k} = \dfrac{n}{k}\binom{n-1}{k-1}$ $\qquad 0 < k \leq n$
3. $\binom{n}{k} = \dfrac{n}{n-k}\binom{n-1}{k}$ $\qquad 0 \leq k < n$
4. $\displaystyle\sum_{i=1}^{n} i = \binom{n+1}{2}$

Bijlage B

Euler-$_\phi$-functie

Lees blz 79-80 in *"Number Theory for Computing", Song Y. Yan.* Van het bewijs op blz 80 lees je deel 2, 3 en 4. Beantwoord daarna volgende vragen.

Oefening 2

Welke bewoordingen horen bij welke uitdrukkingen uit het boek (nrs 1.144 tot 1.149)?

1. *Elk getal n is gelijk aan de som van de Euler-ϕ-functie van elk van zijn delers.*
2. *Elke getal kleiner dan een priemgetal is relatief priem met dat getal.*
3. *Wil je $\phi(72)$ kennen, dan volstaat het $\phi(8)$ en $\phi(9)$ te kennen, omdat $ggd(8,9) = 1$.*
4. *De Euler-ϕ-functie geeft het aantal strikt positieve getallen kleiner dan n dat relatief priem is met n.*

Oefening 3

Beantwoord met ja of neen.

1. *Er werd een bewijs uit het ongerijmde gegeven.*
2. *Gegeven $n \in \mathbb{N}$. Dan telt het getal 1 niet mee om de Euler-ϕ-functie te berekenen.*
3. *Elk getal dat relatief priem is met alle getallen kleiner dan zichzelf, is zelf priem.*

Oefening 4

Bereken, en geef aan welke rekenregels (1.146-1.149) je gebruikte.

1. $\phi(8)$
2. $\phi(97)$
3. $\phi(81)$
4. $\phi(360)$
5. $\phi(56)$

Bijlage C

Binomiale kansverdeling

Op de wip tussen discrete en numerieke wiskunde: de binomiale kansverdeling. Dit stukje theorie is gebaseerd op de telprincipes uit hoofdstuk 3, en legt de link met kansrekenen.

Gegeven een gebeurtenis met een bepaalde kans van "slagen". Bijvoorbeeld: als we een blauwe knikker uit een zak met b blauwe en r rode knikkers willen trekken, is de kans op deze gebeurtenis $\frac{b}{b+r}$. Wat is dan de kans dat we, bij een opeenvolging van n dergelijke gebeurtenissen (dus trekking met teruglegging!) precies k keer "slagen"? Of nog: de kans op k blauwe knikkers?

Daarvoor tellen we het aantal mogelijke uitkomsten met k blauwe en $n-k$ rode knikkers. We tellen eerst de uitkomsten waarbij de blauwe allemaal eerst getrokken werden (we noemen dit voor verdere verwijzing een blauw-roodtrekking). Voor de eerste knikker had je b mogelijkheden, voor de tweede knikker ook b, enzovoort. Voor alle knikkers na de k-de had je r mogelijkheden, die zijn namelijk rood. In totaal heb je dus $b^k \cdot r^{n-k}$ uitkomsten waarbij alle blauwe vooraan in het rijtje blijken te liggen. Om álle mogelijke uitkomsten te tellen, gaan we na hoeveel algemene uitkomsten er horen bij één blauw-roodtrekking. Hiervoor houden we de blauwe knikkers in dezelfde volgorde, maar kiezen we k van de n plaatsjes uit waar we ze over verdelen. De rode knikkers (ook in dezelfde volgorde als in de oorspronkelijke blauw-roodtrekking), krijgen de overige plaatsen toegewezen. Zo komt elke blauw-roodtrekking overeen met $\binom{n}{k}$ algemene oplossingen. Er zijn dus

$$\binom{n}{k} b^k r^{n-k}$$

mogelijke trekkingen met precies k blauwe knikkers. Het totale aantal uitkomsten waarbij het aantal blauwe er niet toe doet, is $(b+r)^n$. De kans op een trekking met k blauwe knikkers is bijgevolg

$$\frac{1}{(b+r)^n} \binom{n}{k} b^k r^{n-k}.$$

Merk op:

$$\begin{aligned}\sum_{k=0}^{n} \frac{1}{(b+r)^n} \binom{n}{k} b^k r^{n-k} &= \sum_{k=0}^{n} \binom{n}{k} \left(\frac{b}{b+r}\right)^k \left(\frac{r}{b+r}\right)^{n-k} \\ &= \left(\frac{b}{b+r} + \frac{r}{b+r}\right)^n \\ &= 1\end{aligned}$$

Inderdaad, tellen we de kansen op 0, 1, 2, ..., n blauwe knikkers samen, dan komt dit uit op 1. Bovenstaande herwerking van de sommatie brengt ook een andere interpretatie van onze berekeningen aan het licht: we kunnen de kans op trekking van n knikkers waarvan exact k blauwe, ook verwoorden in functie van de kans op trekking van 1 blauwe knikker. Deze kans is $\frac{b}{b+r}$, en stellen we in de formule gelijk aan p. De kans op een rode is $\frac{r}{b+r} = 1 - p$.

Stelling. *De kans dat een gebeurtenis zich precies k van de n keer voordoet, als ze een kans heeft om p op 1 keer voor te komen, wordt gegeven door*

$$\binom{n}{k} p^k (1-p)^{n-k}.$$

Bewijs Door bovenstaande redenering. □

Dergelijke kansverdeling komt zeer vaak voor, en wordt de **binomiale kansverdeling** genoemd.

Voorbeeld

Bij een dobbelspel worden de worpen 1 en 6 als winst genoteerd, de andere uitkomsten als verlies. Wat is de kans om in 6 of meer van de 10 worpen winst te behalen?

De kans op winst in één worp is 1/3. De kans op k keer winst in n worpen is

$$\binom{n}{k} \left(\frac{1}{3}\right)^k \left(\frac{2}{3}\right)^{n-k}.$$

Schrijven we dit uit voor $n = 10$ en $k = 6, 7, 8, 9, 10$ dan krijgen we

	$\binom{10}{k}$	1^k	2^{10-k}	$/3^{10}$		
$k = 6$	210	1	16	59049	=	3360/59049
$k = 7$	120	1	8	59049	=	960/59049
$k = 8$	45	1	4	59049	=	180/59049
$k = 9$	10	1	2	59049	=	20/59049
$k = 10$	1	1	1	59049	=	1/59049
totaal						4521/59049

Samen geeft dit een kans van $4521/59049 \approx 7,65\%$ kans om in minstens 60% van de worpen winst te maken.

Bijlage D

Groepen, ringen, velden

Een **groep** is een niet-ledige verzameling $\mathcal{G}$ van elementen waarop een binaire operator $\star$ is gedefinieerd, zó dat volgende eigenschappen gelden:

(1)	$\mathcal{G}$ is gesloten onder $\star$	$\forall a, b \in \mathcal{G} : a \star b \in \mathcal{G}$
(2)	$\star$ is associatief	$\forall a, b, c \in \mathcal{G} : (a \star b) \star c = a \star (b \star c)$ Een groep
(4)	er is een uniek eenheidselement voor $\star$	$\exists e \in \mathcal{G} : \forall a \in \mathcal{G} : a \star e = a = e \star a$
(5)	elk element heeft een invers voor $\star$	$\forall a \in \mathcal{G} : \exists b \in \mathcal{G} : a \star b = e = b \star a$

wordt meestal genoteerd aan de hand van verzameling én operator, dus $< \mathcal{G}, \star >$ of $(\mathcal{G}, \star)$. Als de bewerking duidelijk blijkt uit de contekst, durft men de operator soms weg te laten uit de naamgeving.

Een **commutatieve groep** (of **Abelse groep**) is een groep $(\mathcal{G}, \star)$ waarvoor bovendien commutativiteit van de bewerking $\star$ geldt.

(3)	$\star$ is commutatief	$\forall a, b \in \mathcal{G} : a \star b = b \star a$

Een **eindige** (al dan niet Abelse) **groep** is een (Abelse) groep $(\mathcal{G}, \star)$ waarbij $\mathcal{G}$ eindig is. Het aantal elementen van $\mathcal{G}$ wordt de orde van de groep $(\mathcal{G}, \star)$ genoemd, en noteren we als $|\mathcal{G}|$ of $\sharp(\mathcal{G})$.

Een **ring** is een verzameling $\mathcal{R}$ van minimum twee elementen waarop twee binaire operatoren $\oplus$ en $\odot$ gedefinieerd zijn, zó dat volgende eigenschappen gelden:

(1)	$\mathcal{R}$ is gesloten onder $\oplus$	$\forall a, b \in \mathcal{R} : a \oplus b \in \mathcal{R}$
(2)	de bewerking $\oplus$ is associatief	$\forall a, b, c \in \mathcal{R} : (a \oplus b) \oplus c = a \oplus (b \oplus c)$
(3)	de bewerking $\oplus$ is commutatief	$\forall a, b \in \mathcal{R} : a \oplus b = b \oplus a$
(4)	er is een uniek eenheidselement voor $\oplus$ dit elt. wordt het additief eenheidselt. genoemd, doorgaans genoteerd met 0	$\exists e \in \mathcal{R} : \forall a \in \mathcal{R} : a \oplus e = a = e \oplus a$
(5)	elk element heeft een invers voor $\oplus$ dit elt. wordt 't additief invers van a genoemd, doorgaans genoteerd als $-a$	$\forall a \in \mathcal{R} : \exists b \in \mathcal{R} : a \oplus b = e = b \oplus a$
(1')	$\mathcal{R}$ is gesloten onder $\odot$	$\forall a, b \in \mathcal{R} : a \odot b \in \mathcal{R}$
(2')	de bewerking $\odot$ is associatief	$\forall a, b, c \in \mathcal{R} : (a \odot b) \odot c = a \odot (b \odot c)$
(6')	de bewerking $\odot$ is distributief tov $\oplus$	$\forall a, b, c \in \mathcal{R} : a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

Een **commutatieve ring** is een ring $(\mathcal{R}, \oplus, \odot)$ met bijkomende eigenschap

(3')	de bewerking $\odot$ is commutatief	$\forall a, b \in \mathcal{R} : a \odot b = b \odot a$

Een **ring met eenheidselement** is een ring $(\mathcal{R}, \oplus, \odot)$ met bijkomende eigenschap

(4')	er is een uniek eenheidselement voor $\odot$ dit elt. wordt het multiplicatief eenheidselt. genoemd, doorgaans genoteerd met 1	$\exists \mathbf{1} \in \mathcal{R} : \forall a \in \mathcal{R} : a \odot \mathbf{1} = a = \mathbf{1} \odot a$

Een **veld** is een commutatieve ring met eenheidselement met bijkomende eigenschap

(5')	elk element ($\neq 0$) heeft een invers voor $\odot$ dit elt. wordt het multiplicatief invers van a genoemd, doorgaans genoteerd als a^{-1}.	$\forall a \in \mathcal{G} : \exists b \in \mathcal{G} : a \odot b = e = b \odot a$

Een **eindig veld** is een veld waarvan de verzameling een eindig aantal elementen bezit.

Stelling D.1. *Er bestaat een veld van de orde q als en slechts als q een priemmacht is ($q = p^r$, p priem en $r \in \mathbb{N}$). Bovendien bestaat er slechts één veld van die orde (eventueel door herschikken van elementen te bekomen). Zulk eindig veld wordt dikwijls een* **Galoisveld** *genoemd, en noteren we met* $\mathbf{GF}(q)$ *of* $\mathbb{F}(q)$.

Voorbeeld De verzamelingen $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ (met bewerkingen) zijn oneindige velden; $\mathbb{Z}$ is een ring; en $\mathbf{GF}(5) = \{0, 1, 2, 3, 4\} = \mathbb{Z}/_{5\mathbb{Z}}$ is een eindig veld.

Bijlage E

Machten modulo n

MODULO 4

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	0	0	0	0	0	0	0
3	1	3	1	3	1	3	1

MODULO 5

0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
2	4	3	1	2	4	3	1	2
3	4	2	1	3	4	2	1	3
4	1	4	1	4	1	4	1	4

MODULO 6

0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
2	4	2	4	2	4	2	4	2	4
3	3	3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4	4	4
5	1	5	1	5	1	5	1	5	1

MODULO 7

0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2	6	4	5
4	2	1	4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4	6	2	3
6	1	6	1	6	1	6	1	6	1	6

MODULO 8

0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
2	4	0	0	0	0	0	0	0	0	0	0
3	1	3	1	3	1	3	1	3	1	3	1
4	0	0	0	0	0	0	0	0	0	0	0
5	1	5	1	5	1	5	1	5	1	5	1
6	4	0	0	0	0	0	0	0	0	0	0
7	1	7	1	7	1	7	1	7	1	7	1

MODULO 9

0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	7	5	1	2	4	8	7	5	1	2
3	0	0	0	0	0	0	0	0	0	0	0	0
4	7	1	4	7	1	4	7	1	4	7	1	4
5	7	8	4	2	1	5	7	8	4	2	1	5
6	0	0	0	0	0	0	0	0	0	0	0	0
7	4	1	7	4	1	7	4	1	7	4	1	7
8	1	8	1	8	1	8	1	8	1	8	1	8

MODULO 10

0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	6	2	4	8	6	2	4	8	6	2	4
3	9	7	1	3	9	7	1	3	9	7	1	3	9
4	6	4	6	4	6	4	6	4	6	4	6	4	6
5	5	5	5	5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6	6	6	6	6
7	9	3	1	7	9	3	1	7	9	3	1	7	9
8	4	2	6	8	4	2	6	8	4	2	6	8	4
9	1	9	1	9	1	9	1	9	1	9	1	9	1

MODULO 11

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1	2	4	8	5	10
3	9	5	4	1	3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1	6	3	7	9	10
7	5	2	3	10	4	6	9	8	1	7	5	2	3	10
8	9	6	4	10	3	2	5	7	1	8	9	6	4	10
9	4	3	5	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1	10	1	10

MODULO 12

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	4	8	4	8	4	8	4	8	4	8	4	8	4
3	9	3	9	3	9	3	9	3	9	3	9	3	9	3	9
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	1	5	1	5	1	5	1	5	1	5	1	5	1	5	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	1
8	4	8	4	8	4	8	4	8	4	8	4	8	4	8	4
9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
10	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1

MODULO 13

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	1	2	4	8	3	6
3	9	1	3	9	1	3	9	1	3	9	1	3	9	1	3	9
4	3	12	9	10	1	4	3	12	9	10	1	4	3	12	9	10
5	12	8	1	5	12	8	1	5	12	8	1	5	12	8	1	5
6	10	8	9	2	12	7	3	5	4	11	1	6	10	8	9	2
7	10	5	9	11	12	6	3	8	4	2	1	7	10	5	9	11
8	12	5	1	8	12	5	1	8	12	5	1	8	12	5	1	8
9	3	1	9	3	1	9	3	1	9	3	1	9	3	1	9	3
10	9	12	3	4	1	10	9	12	3	4	1	10	9	12	3	4
11	4	5	3	7	12	2	9	8	10	6	1	11	4	5	3	7
12	1	12	1	12	1	12	1	12	1	12	1	12	1	12	1	12

MODULO 14

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	2	4	8	2	4	8	2	4	8	2	4	8	2	4	8
3	9	13	11	5	1	3	9	13	11	5	1	3	9	13	11	5	1
4	2	8	4	2	8	4	2	8	4	2	8	4	2	8	4	2	8
5	11	13	9	3	1	5	11	13	9	3	1	5	11	13	9	3	1
6	8	6	8	6	8	6	8	6	8	6	8	6	8	6	8	6	8
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
9	11	1	9	11	1	9	11	1	9	11	1	9	11	1	9	11	1
10	2	6	4	12	8	10	2	6	4	12	8	10	2	6	4	12	8
11	9	1	11	9	1	11	9	1	11	9	1	11	9	1	11	9	1
12	4	6	2	10	8	12	4	6	2	10	8	12	4	6	2	10	8
13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1

MODULO 15

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8
3	9	12	6	3	9	12	6	3	9	12	6	3	9	12	6	3	9	12
4	1	4	1	4	1	4	1	4	1	4	1	4	1	4	1	4	1	4
5	10	5	10	5	10	5	10	5	10	5	10	5	10	5	10	5	10	5
6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
7	4	13	1	7	4	13	1	7	4	13	1	7	4	13	1	7	4	13
8	4	2	1	8	4	2	1	8	4	2	1	8	4	2	1	8	4	2
9	6	9	6	9	6	9	6	9	6	9	6	9	6	9	6	9	6	9
10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1	11
12	9	3	6	12	9	3	6	12	9	3	6	12	9	3	6	12	9	3
13	4	7	1	13	4	7	1	13	4	7	1	13	4	7	1	13	4	7
14	1	14	1	14	1	14	1	14	1	14	1	14	1	14	1	14	1	14

MODULO 16

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	9	11	1	3	9	11	1	3	9	11	1	3	9	11	1	3	9	11	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	9	13	1	5	9	13	1	5	9	13	1	5	9	13	1	5	9	13	1
6	4	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	1	9	1	9	1	9	1	9	1	9	1	9	1	9	1	9	1	9	1
10	4	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	9	3	1	11	9	3	1	11	9	3	1	11	9	3	1	11	9	3	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	9	5	1	13	9	5	1	13	9	5	1	13	9	5	1	13	9	5	1
14	4	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	1	15	1	15	1	15	1	15	1	15	1	15	1	15	1	15	1	15	1

MODULO 17

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1	2	4	8	16	15
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	3	9	10	13	5
4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1	4
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1	5	8	6	13	14
6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1	6	2	12	4	7
7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1	7	15	3	4	11
8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1	8	13	2	16	9
9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1	9	13	15	16	8
10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1	10	15	14	4	6
11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1	11	2	5	4	10
12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1	12	8	11	13	3
13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1	13
14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1	14	9	7	13	12
15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1	15	4	9	16	2
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16

Bijlage F

Oefeningen

OEFENINGEN BIJ HOOFDSTUK 1

Oefening 101

Toon aan dat voor de getallen van Fibonacci (dit is de reeks $(a_n)_{n\in\mathbb{N}}$ met $\underline{a_0 = 0}$, $a_1 = 1$ en $a_{n+2} = a_{n+1} + a_n$) volgende gelijkheid geldt:

$$a_n = a_r a_{n-r-1} + a_{r+1} a_{n-r}, \forall r, 0 \leq r \leq n-1.$$

Gebruik inductie op r en geef voldoende tekst en uitleg bij je bewijs.

OEFENINGEN BIJ HOOFDSTUK 2

Oefening 201

Gegeven de logische functie γ en de verzameling logische functies Γ. Ga na of γ logisch gevolg is van Γ ($\Gamma \models \gamma$). Geef duidelijk je redenering en conclusie weer met — indien van toepassing — een weerlegging voor de uitspraak $\Gamma \models \gamma$.

1. $\gamma = \neg m \to (\neg f \vee p)$
   $\Gamma = \{(a \wedge q) \to m, (f \to q) \wedge (\neg p \to a)\}$
2. $\gamma = r \to (n \vee t)$
   $\Gamma = \{r \to (c \vee l), \neg c \to \neg n, \neg t \to \neg l\}$
3. $\gamma = s$
   $\Gamma = \{p \vee q, p \to r, p \to (q \vee \neg r), \neg q \vee \neg s\}$

OEFENINGEN BIJ HOOFDSTUK 3

Oefening 301

Gegeven een volledige ongerichte graaf op 200 toppen. (Een volledige graaf heeft tussen elke twee toppen een verbinding.) We kleuren R toppen rood, B toppen blauw en de rest wordt wit. Hoeveel verbindingen zijn er

1. *met twee rode eindpunten*
2. *met twee blauwe eindpunten*
3. *met twee witte eindpunten*
4. *met een rood en een blauw eindpunt*
5. *met een blauw en een wit eindpunt*
6. *met een wit en een rood eindpunt.*

Oefening 302

(Hier heb je bijlage C voor nodig.) *Rangschik de gegeven spelen op winstkans en argumenteer. Vooraan in het lijstje zet je het spel waarbij je - volgens de kansrekening - minst snel blut bent. Geef de winstkansen en de redenering die je gebruikte.*

1. *Uit een kaartspel van 52 kaarten worden er 2 getrokken. Twee 'prenten' (boer, heer, dame uit één van de vier kleuren) levert je winst. (Hint: kans = aantal goede uitkomsten / aantal mogelijke uitkomsten.)*
2. *Er wordt 5 maal geworpen met een dobbelsteen met 12 (twaalf!) zijden. Heb je precies 2 maal het getal 1 gegooid, dan heb je winst.*
3. *Zelfde spel als hierboven, maar je wint als je precies 3 maal het getal 12 gooide.*

Oefening 303

Gegeven een structuur van punten en rechten. We weten:

- *Er zijn* 273 *punten.*
- *Er zijn* 273 *rechten.*
- *Door elk punt gaan precies* 17 *rechten.*
- *Op elke rechte liggen precies* 17 *punten.*

We kleuren een deel van de punten en rechten rood, het andere deel kleuren we / laten we zwart. Hierbij gelden volgende regels:

- *Als we een punt rood kleuren, kleuren we precies* 5 *rechten door dit punt rood.*
- *Als we een rechte rood kleuren, kleuren we precies* 5 *punten op deze rechte rood.*
- *Op een zwarte rechte wordt precies 1 punt rood gekleurd.*
- *Door een zwart punt gaat precies 1 rode rechte.*

Als je evenveel punten als rechten rood kleurt, hoeveel punten kleurde je dan?

Maak een duidelijke schets bij je redenering.

Oefening 304

1. *Geef het aantal deelverzamelingen van een verzameling met n elementen, en toon aan.*

2. *Bewijs dat* $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n}$ *gelijk is aan* 2^n.
3. *Bewijs dat* $r\binom{n}{r} = n\binom{n-1}{r-1}$.
4. *Bewijs dat* $\sum_{r=1}^{n} r\binom{n}{r} = n \cdot 2^{n-1}$.

Hint: los de oefeningen in de aangegeven volgorde op.

Oefening 305

Op school wordt er tijdens de middagpauze (maandag, dinsdag, donderdag en vrijdag) altijd gesport. De leerlingen kunnen kiezen uit 3 sporten (voetbal, pingpong, atletiek).

1. *Op hoeveel manieren kan Piet zijn sporten kiezen, zodat hij niet moet voetballen? (Merk op: pingpong op maandag en atletiek op dinsdag is niet hetzelfde als atletiek op maandag en pingpong op dinsdag.)*
2. *Op hoeveel manieren kan Els haar sporten kiezen, als ze geen speciale wensen heeft?*
3. *Op hoeveel manieren kan Jan zijn sporten kiezen, als hij die week elke sport minstens één keer wil meedoen?*
4. *Controleer of de aantallen kloppen door middel van een venndiagram (tekening van verzamelingen), waarbij je elke verzameling het etiket "*zonder sport ...*" geeft.*

Oefening 306

1. *Hoeveel deelverzamelingen van* $\{1, 2, 3, \ldots, 11\}$ *bevatten minstens 1 even getal?*
2. *Gegeven* $S = \{1, 2, \ldots, 30\}$. *Hoeveel deelverzamelingen van kardinaliteit 5 zijn er, waarvan het kleinste getal het getal* 8 *is?*
3. *Als de verzameling* B *64 deelverzamelingen heeft van oneven kardinaliteit; wat is* $|B|$ *dan?*
4. *Bepaal alle mogelijke waarden voor* n *in volgende uitspraak: 'een regelmatige* n*-hoek heeft evenveel zijden als diagonalen'.*
5. *Hoeveel elementen moet een deelverzameling* S *van*

$$\{1, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 16, 18\}$$

ten minste bevatten om zeker te zijn dat er 2 elementen in deze deelverzameling zitten waarvan de som 20 *is?*

OEFENINGEN BIJ HOOFDSTUK 4

Oefening 401

Zoek de coëfficiënt van x^6 in de ontwikkeling van de functie $\dfrac{1}{x^2-5x+6}$.

Oefening 402

Gegeven s_0, en $s_n = as_{n-1} + b$ voor $n \geq 1$ met a en b constanten, en $a \neq 1$.

1. *Als S de genererende functie is voor de rij (s_n), toon dan aan dat $S = s_0 + axS + \dfrac{bx}{1-x}$.*
2. *Toon aan dat $s_n = \left(s_0 + \dfrac{b}{a-1}\right) a^n - \dfrac{b}{a-1}$ voor $n \geq 0$.*

Oefening 403

1. *Zoek het aantal oplossingen in $\{6,7,8,9\}$ van de vergelijking $a+b+c+d = 33$. Hierbij is de oplossing $(a,b,c,d) = (7,8,9,9)$ verschillend van de oplossing $(a,b,c,d) = (8,9,7,9)$.*
2. *Zelfde vraag, maar nu zoek je het aantal 'ongeordende' oplossingen $\{a,b,c,d\}$. Hierbij is de oplossing $\{a,b,c,d\} = \{7,8,9,9\}$ gelijk aan de oplossing $\{a,b,c,d\} = \{8,9,7,9\}$.*
3. *Geef aan hoe / ga na of je van het aantal dat je onder de tweede vraag vond, het aantal onder de eerste vraag kan vinden.*

Hint: $\left(\dfrac{1}{1-x}\right)^n = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k$.

Oefening 404

Een computer aanvaardt als paswoord elke rij cijfers (cijfer$\in \{0,1,\ldots,8,9\}$) die een even aantal maal het cijfer 3 bevat. Noem a_n het aantal paswoorden van lengte n. Bereken a_1 en a_2, en bewijs dat de recurrente betrekking van a_n gegeven wordt door $a_n = 8a_{n-1} + 10^{n-1}$.

Oefening 405

Een rij $(x_n)_{n \in \mathbb{N}}$ wordt gedefinieerd door de startwaarden $x_0 = x_1 = 1, x_2 = 2$ en de recurrente betrekking

$$x_{n+3} = 3x_{n+1} + 2x_n.$$

Merk op: de index van het linkerlid is wel degelijk $n+3$. Geef een rechtstreekse formule voor de algemene term x_n van de rij; $n \geq 3$.

Oefening 406

Zoek een rechtstreekse formule voor de algemene rijterm a_n, als je weet dat

$$\begin{array}{lcll} a_0 & = & 0 & \\ a_1 & = & 1 & \\ a_2 & = & 2 & \\ 2 \cdot a_{n+3} & = & a_{n+2} + 2a_{n+1} - a_n, & n \geq 0 \end{array}$$

Doe dit op twee manieren: via de voortbrengende functie $M = \sum a_n x^n$ en via de karakteristieke vergelijking van de recurrente betrekking (laatste paragraaf van hoofdstuk 4).

Oefening 407

Elke dag op weg naar huis koop je juist 1 ding uit de volgende:

```
appel      1 euro
peer       1 euro
mango      2 euro
banaan     2 euro
avocado    2 euro
ananas     3 euro
```

Geef het aantal s_n van verschillende volgordes waarbij je precies n euro spendeert. (Beginwaarden en recurrente betrekking.)

OEFENINGEN BIJ HOOFDSTUK 5

Oefening 501

Geef de oplossingen in $\boldsymbol{Z}$ van volgende vergelijkingen:

1. $1734\ x + 1955\ y = 340$
2. $6096\ x + 68004\ y = 240$

Oefening 502

Bij de uitwerking van een oefening waarvoor de Chinese reststelling gebruikt werd, komt op een gegeven moment volgende gelijkheid naar boven:

$$d \cdot 6 \cdot 48 \cdot 47 \cdot 26 \equiv 26 \ mod\ 43$$

Het linkerlid is wel degelijk een product van 5 factoren. Bereken de kleinst mogelijke waarde voor d, maar ZONDER zakrekenmachine. Dit wil zeggen: schrijf alle *tussenstappen, gebruik* nooit *getallen van meer dan 3 cijfers, dus werk producten ook niet uit als het niet hoeft. (Je mag je zakrekenmachine wel houden als extra steuntje voor het zelfvertrouwen, maar foefel geen grote getallen stiekem weg door stappen over te slaan; dat valt op!)*

Oefening 503

Bereken $z = 219 \cdot 42$ op een computer die enkel de getallen $\{0, 1, \cdots, 29\}$ kan voorstellen. Zelfde opmerking als bij oefening hierboven: vereenvoudigen in plaats van grote getallen gebruiken! Voor je eindresultaat mag je uiteraard wel weer grotere getallen gebruiken.

OEFENINGEN BIJ HOOFDSTUK 6

Oefening 601

Bereken onderstaande uitdrukkingen indien eenduidig gedefinieerd. Indien dat niet het geval is, geef dan aan wat er aan de hand is.

1. $ind_{3,11}(6)$
2. $ind_{3,11}(5)$
3. $ind_{7,11}(2)$
4. $ind_{7,11}(1)$

Twijfel je aan de notatie, leid de juiste betekenis dan af uit de gelijkheid $ind_{2,13}(5) = 9$.

OEFENINGEN BIJ HOOFDSTUK 7

Oefening 701

Ontbind (zover mogelijk) in factoren over het aangegeven veld. Geef aan hoe je weet dat de bekomen ontbinding volledig is (d.w.z. niet verder ontbonden kan worden).

1. $1 + x + x^5$ *over* $\boldsymbol{Z}/_{2\boldsymbol{Z}}$
2. $1 + x^4 + x^5$ *over* $\boldsymbol{Z}/_{2\boldsymbol{Z}}$
3. $x^6 + x^5 - x^4 - x^3 - x - 1$ *over* $\boldsymbol{Z}/_{3\boldsymbol{Z}}$
4. $x^5 + 2x^4 - 2x^3 - x^2 - 2x + 2$ *over* $\boldsymbol{Z}/_{5\boldsymbol{Z}}$
5. $x^5 - x^4 + x^3 - 2x^2 - 2x + 2$ *over* $\boldsymbol{Z}/_{5\boldsymbol{Z}}$

Oefening 702

Gegeven het veld $\mathbf{GF}(16)$ *voortgebracht door de functie* $\alpha^4 + \alpha + 1$. *Toon aan dat de verzameling* $\{0, \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{14}\}$ *gelijk is aan* $\mathbf{GF}(16)$. *Schrijf hiervoor alle machten van* α *in de vorm van een veelterm in* α, *waarbij de veelterm coëfficiënten in* $\boldsymbol{Z}/_{2\boldsymbol{Z}}$ *heeft, en graad kleiner dan 4. Werk in twee kolommen: links staan* $0, \alpha^0, \alpha^1, \ldots$; *rechts staan de veeltermnotaties.*

In de derde kolom schrijf je nu de waarde van $1 + y$, *met* y *het getal uit de eerste / tweede kolom. Gebruik voor deze derde kolom weer de machtnotatie, dus* $1 + \alpha^i = \alpha^j$, *met* i *gaande van 0 tot 14. (Hier moet je niet veel berekenen, maar eerder opzoekwerk verrichten in de andere kolommen!)*

Met de opgestelde tabel (de Zech log-tabel) kan je nu berekeningen in $\mathbf{GF}(16)$ *eenvoudiger laten verlopen. Bereken volgende uitdrukkingen, en gebruik daarbij* enkel de eerste en laatste kolom van de opgestelde tabel, *en* niet *meer de voortbrengende functie* $\alpha^4 + \alpha + 1$. *Je oplossing blijft staan in de vorm* α^k. *Uiteraard vermeld je de genomen tussenstappen.*

1. $\alpha^2 \cdot \alpha^3$
2. $1 + \alpha^3$
3. $\alpha^5 + \alpha^8$
4. $\alpha^5 + \alpha^8 + \alpha^9$
5. $\alpha^4 + \alpha^7 + \alpha^9 + \alpha^{12}$

OEFENINGEN BIJ HOOFDSTUK 8

Oefening 801

Bepaal de transitieve sluiting van de gerichte graaf op vijf toppen waarvan de verbindingen hieronder gegeven zijn. Doe dit zowel via schets als via wiskundige berekening.

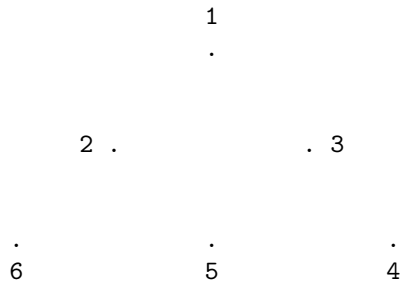
$$(5,2) \qquad (2,4) \qquad (4,1) \qquad (1,3) \qquad (5,3)$$

Oefening 802

Gegeven een gerichte multigraaf op 6 toppen. Bepaal het aantal paden van lengte 4 vanuit punt 1 naar de andere punten. Doe dit op twee manieren:

1. *via wiskundige berekening (gebruik zo weinig mogelijk rekenwerk!).*
2. *via schets: teken de verbindingen tussen de reeds getekende punten (neem de schets over op je antwoordblad), en geef ze de bijhorende letter. Schrijf daarna alle gevonden paden van lengte 4 vanuit punt 1 naar punten $2, \ldots, 6$ op (schrijf de letters van de gevolgde verbindingen op).*

$a(1,3)$ $b(1,3)$ $c(3,1)$ $d(1,2)$ $e(2,6)$ $f(6,5)$ $g(5,2)$ $h(3,4)$ $i(4,2)$



Oefening 803

Bereken de kortste afstanden tussen de vijf knopen van de gewogen graaf G, *met verbindingen*

$$(1,2),(2,4),(3,2),(4,3),(4,2),(4,1),(4,5),(5,3),(5,4),(5,2),(5,1)$$

en respectieve gewichten

$$3 \quad 3 \quad 1 \quad 4 \quad 7 \quad 9 \quad 5 \quad 6 \quad 6 \quad 8 \quad 7.$$

Geef een beetje toelichting bij de gebruikte berekeningsmethode, en vergeet het antwoord niet te formuleren.

Oefening 804

Gegeven een gerichte en gewogen graaf. Gevraagd: voor elk koppel knopen (x, y) het gewicht van het minst wegende pad van x naar y. Er is echter een bijkomende eigenschap van de graaf waarmee je rekening dient te houden: elke knoop $(\neq x, \neq y)$ die je op je pad tegenkomt, draagt ook *bij tot het totale gewicht van het pad; de bijdrage van elke knoop is 1. (Beschouw de graaf als een voorstelling van een spoorwegennet, waarbij 'een knoop passeren' gelijk staat met 'een tijdje stilstaan in een station'.) Gebruik voor je antwoord geen schets (dit mag enkel als controlemiddel gebruikt worden). Als $x = y$, geef je het gewicht van de minst wegende niet-triviale cykel (een cykel is triviaal als hij geen verbindingen bevat). Hierbij de verbindingen en hun respectieve gewichten:*

$$(1,2),(1,3),(1,4),(2,3),(2,5),(3,4),(4,5),(5,2),(5,1)$$

$$3 \quad 7 \quad 8 \quad 2 \quad 7 \quad 2 \quad 2 \quad 6 \quad 1.$$

Inhoudsopgave

Bibliografie

[1] Thomas H. Cormen et al. *Introduction to Algorithms.* The MIT Press, 2nd edition, 2001.

[2] Frank De Clerck. *Diskrete Wiskunde.* Cursus 1e bachelor informatica aan Universiteit Gent, 2005.

[3] John A. Dossey et al. *Discrete Mathematics.* Pearson Addison Wesley, 5th edition, 2006.

[4] Ralph P. Grimaldi. *Discrete and Combinatorial Mathematics, An Applied Introduction.* Pearson Addison Wesley, 5th edition, 2004.

[5] William Stallings. *Crypthography and Network Security: Principles and Practice.* Prentice Hall, 4d edition, 2006.

[6] Rudy Stoop. *Algoritmen en Gegevensstructuren.* Cursussen 3e bachelor en master in de industriële wetenschappen in informatica aan Hogeschool Gent, 2005.

[7] John Truss. *Discrete Mathematics for Computer Scientists.* Addison Wesley, 2nd edition, 1999.

[8] Song Y. Yan. *Number Theory for Computing.* Springer, 2nd edition, 2002.

Discrete wiskunde: hints bij oefeningen

Zeer belangrijke opmerking voor je de hints doorneemt

De hints bij de oefeningen zijn NIET bedoeld als lectuur voor studenten die hun theorie nog niet hebben geblokt, en nog niet geconcentreerd gezocht hebben op hun oefeningen.

Doe je dit WEL, dan zijn de gevolgen volledig voor eigen rekening: je beneemt jezelf voor altijd de kans om ervaring op te doen bij het oplossen van het voorgelegde vraagstuk, en deze kans is eenmalig. Immers, eens de hint gelezen is, kan je niet meer de voldoening voelen van er zelf te zijn opgekomen. Of het inzicht verwerven dat je oorspronkelijke redenering niet waterdicht was.

Wees daarom zuinig op het gebruiken van de hints: lees enkel de hint bij de oefening waaraan je bezig bent geweest; deel ze niet zomaar uit aan nieuwe studenten (die krijgen ze op tijd en stond), en besef dat een hint iets anders is dan een mooi uitgeschreven oplossing. Het is enkel bedoeld als aanzet om toch zelf verder te kunnen.

Veel succes toegewenst,
en opmerkingen over deze hints altijd welkom op leen.brouns@ugent.be.

L. Brouns

februari 2014

Hoofdstuk 1: Basisbegrippen

1.4 hint Ga nauwkeurig *elke* stap uit het bewijs na, en formuleer het equivalent voor $n = 3$ en $n = 4$. Bij stap (2) zou het moeten mislopen voor $n = 4$. Indien niet, dan heb je het oorspronkelijke bewijs niet door (dan zitten er gaten in je redenering).

1.5 hint Probeer dingen uit met $\sqrt{2}$ en $\sqrt{3}$ of hun tegengestelden.

1.6 hint Herschrijf $u = (a + b) \bmod n$ als $(a + b) + kn$, waarbij k een niet nader bepaald geheel getal is. Doe hetzelfde voor $a \bmod n$ en $b \bmod n$, en toon dan aan dat het linkerlid *congruent* is met het rechterlid (d.w.z. op een veelvoud van n na gelijk).

Hoofdstuk 2: Inleiding tot logica

2.2 hint Werk zoals op blz 23: schrijf de uitdrukking op één lijn, en doorstreep de kolom(men) die je net gebruikt hebt om een nieuwe kolom in te vullen. Dit gaat het snelst.

2.4 hint Bepaal voor elke mogelijke toekenning van waarden aan de propositionele variabelen de waarde van beide formules. Deze zouden voor elke toekenning moeten overeenkomen.

2.7 hint Bedek de 1-en uit het schema met zo groot mogelijke vierkanten of rechthoeken, waarvan de zijden een macht van 2 zijn. Overlapping mag (en moet, want dat vergroot een van beide vierkanten/rechthoeken).

Hoofdstuk 3: Tellen

3.1 hint Doe deze oefening eerst met 3 of 4 getrouwde stellen; dat controleert makkelijker.

3.2 hint Teken alle congruentieklassen modulo 7. Vul deze op de slechtst mogelijke manier op: stel het bereiken van de voorwaarde (= 10 die tot dezelfde congruentieklasse behoren) zo lang mogelijk uit. Aan hoeveel getallen zit je dan?

3.3 hint Werk meetkundig. Verdeel de driehoek in stukjes met zijde $\frac{1}{2}$.

3.5 hint Typische oefening om eerst uit te proberen met klein aantal pingpongende vrienden, en dan te extrapoleren.

3.7 hint Teken 9 lege plaatsen (= liggende streepjes), voor elk teken eentje. Zet daaronder de verschillende mogelijkheden (of sneller: het aantal verschillende mogelijkheden) voor elke lege plaats.

3.8 hint Teken 3 lege plaatsen, voor elk cijfer in het te vormen getal eentje. Zet daaronder het aantal verschillende mogelijkheden. Voor deel 2 en 3 van de vraag zet je ook best de mogelijkheden zelf in een kolommetje; niet enkel het aantal mogelijkheden.

3.9 hint Deel 2 van de oefening: splits op in deelgevallen. Schrijf uit hoeveel knikkers elke jongen krijgt, en tel (voor dat specifieke geval) het aantal mogelijkheden.

3.11 hint Teken 4 lege plaatsen, voor elk cijfer eentje. Zet daaronder de cijfers die op die plaats kunnen komen (niet enkel het *aantal* cijfers), startend onder het linkerstreepje. Let op, de keuze van het tweede cijfer hangt af van de keuze van het eerste cijfer, dus splits dat op!

3.13 hint Start met het tekenen van 12 lege plaatsen. Vul je dit in met kleuren, dan zie je dat je beter niet van links naar rechts opvult, maar eerst 4 rode rozen plant - dus plaatsen uitkiest. Dus zit je op het spoor van de combinaties (kies 'n groepje van 4 uit 12 beschikbare plaatsen). Werk daarop verder.

3.14 hint Start met het tekenen van 7 lege plaatsen, voor elke letter een. Zet daaronder het aantal mogelijke letters waaruit nog gekozen kan worden. Beschouw de drie A's eerst als drie verschillende mogelijkheden. Daarna zorg je dat dit teveel aan oplossingen verrekend wordt.

3.15 hint Typische oefening om eerst met een kleiner gegeven te starten (op elke helft 1 tot 3 stippen in plaats van 0 tot 6).

3.16 hint Splits op in gevallen, naargelang je de kooien leeg laat dan wel aan wolven resp. schapen toewijst.

3.19 hint Dubbele telling: maak drie verzamelingen voor respectievelijk punten, rechten, vlakken. Duid alle gegevens nauwkeurig aan, en vul de ontbrekende gegevens aan aan de hand van de werkwijze op blz 51.

Hoofdstuk 4: Voortbrengende functies

4.1 hint Stel $g(x)$ gelijk aan $a_0 + a_1x + a_2x^2 + a_3x^3 + ...$, werk het linkerlid uit, en stel beide leden gelijk aan elkaar. Hieruit volgen $a_0, a_1, ...$

4.3 hint Werk de eerste 5 termen uit.

4.7 hint

1. **Eerste hint** De vraag moet beantwoord worden voor n willekeurig. Begin met het antwoord voor $n = 0$, $n = 1$, $n = 2$. De eerste 2 zijn triviaal, voor $n = 2$ moet je werken zoals bij de teloefeningen: teken twee liggende streepjes (eentje voor elk cijfer van de code), en zet onder het eerste welke mogelijkheden er zijn. Daarna zet je voor het tweede ook welke mogelijkheden er zijn; let op: dat hangt af van je keuze voor het eerste cijfer! Dit geeft in totaal $8 \cdot 2 + 2 \cdot 8 = 32$ mogelijkheden. Pas nu recursie toe.
2. **Tweede hint** Stel dat je c_{n-1} kent; dit is het aantal codewoorden van lengte $n - 1$. Dan ken je ook het aantal niet-codewoorden van lengte $n - 1$. Stel nu een codewoord van lengte n op: voeg aan een serie van $n - 1$ cijfers nog een n-de cijfer toe. (Is de oorspronkelijke serie een codewoord? Dan voeg je *geen* 3 of 7 toe. In het andere geval net wel.)

Hoofdstuk 6: Diophantische vergelijkingen: niet-lineair

6.1 hint Gevraagd: 4^{35} mod 17. Gebruik de kleine stelling van Fermat: $a^{p-1} \equiv 1 \bmod p$ maar ga eerst de voorwaarden van deze stelling na! Schrijf 4^{35} als $4^{16} \cdot 4^{16} \cdot 4^3$ en werk zorgvuldig uit (kan je elke stap verantwoorden?).

6.2 hint Analoog aan oefening 1, al is 693 duidelijk niet priem. Gebruik dus een andere stelling.

Hoofdstuk 7: Eindige velden

7.6 hint De verzameling $\boldsymbol{Z}/_{2\boldsymbol{Z}}$ heeft slechts 2 elementen: 0 en 1. De enige mogelijke *lineaire* factoren zijn dus x en $x + 1$ (nl. 0 respectievelijk 1 is nulpunt van de gegeven functie!). Gebruik de methode van Horner om die lineaire factor snel uit te delen (tenzij je op zicht dingen buiten haakjes kan zetten). Vind je geen lineaire factoren (meer), dan ga je verder met tweede- (of derde-) graadsfactoren. Je stelt een vorm voor die factoren voorop, met onbekende coëfficiënten, en bepaalt dan de onbekenden door middel van gelijkstelling. (In concreto, voor oefening 5: zoek a, b, c, d, e, f in $(a + bx + cx^2)(d + ex + fx^2) = 1 + x + x^2 + x^3 + x^4$. Uiteraard mag je onmiddellijk $a = d = 1$ stellen!)

Examenoefeningen

101 hint Voor een bewijs met inductie leg je eerst duidelijk vast op *welke* variabele je inductie toepast, en wat (in de inductiestap) de hypothese is (dus waarop je mag steunen) en wat het te bewijzen is.

201 hint Start met op je (klad)papier de semantische tableaus van de basisbewerkingen te schrijven (en controleer deze goed). Bij de uitwerking van het semantische tableau voor de opgave, vervang je *eerst* de uitdrukkingen waarvoor *geen* opsplitsing nodig is (en doorstreep die dan, van zodra ze verwerkt zijn). Vergeet niet te formuleren wat dit semantische tableau je nu leert!

302 hint Hier heb je bijlage C voor nodig; dat hebben we niet gezien in jaargang 2007-2008.

303 hint Dubbele telling: verdeel elke verzameling in een rode en zwarte helft. De orde van de verzameling is gekend, dus als je α punten rood kleurt, ken je ook het aantal zwarte!

304 hint

1. Bepaal voor elk element of het al dan niet tot de deelverzameling behoort (= 2 mogelijkheden). Combineer al deze mogelijkheden met het juiste telprincipe.
2. Hier staan alle deelverzamelingen van bepaalde grootte-orde van een verzameling van n elementen vermeld.
3. Schrijf combinaties aan de hand van faculteiten; is rekenwerk.
4. Sommeer beide leden over r=1,...,n. Het rechterlid schrijf je voluit; dit zou je moeten doen denken aan deel 2. Gebruik deel 2 dus om tot de verkorte notatie te komen.

401 hint Ontbind in partieelbreuken.

402 hint

1. Werkwijze zoals in cursus.
2. Heb je al inductie geprobeerd? (Formuleer het te bewijzen en het te gebruiken gedeelte zorgvuldig; de rest volgt dan vanzelf.)

404 hint Zie oefening 6 uit hoofdstuk 4.

501 hint Bij deze oefeningen altijd goed nakijken of er een oplossing in $\boldsymbol{Z}$ dan wel $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ gevraagd wordt. Controleer je antwoord, en formuleer het netjes!

601 hint Stel tabellen op voor de discrete logaritmen.

702 hint Volg de instructies nauwkeurig (dat komt neer op rekenwerk). Voor het laatste deel:

$\alpha^2 \cdot \alpha^3$	$= \alpha^5$
$1 + \alpha^3$	zoek op in zelfopgestelde tabel
$\alpha^5 + \alpha^8$	zet α^5 buiten haakjes, en zoek de overblijvende factor op in de tabel
$\alpha^5 + \alpha^8 + \alpha^9$	neem telkens 2 termen samen, en vervang $1 + \alpha^i$ door opzoekwerk in de tabel

80. hint Vergeet bij deze oefeningen het woordje uitleg en het besluit niet. Enkel matrices met getallen in is niet voldoende.

Discrete wiskunde: oplossingen van oefeningen

Zeer belangrijk voor je de oplossingen doorneemt

Meer nog dan bij de hints, geldt hier het principe: beter 1 geprobeerde oefeningen, dan 10 gelezen oplossingen. Laat je niet te snel verleiden!

Veel succes,

L. Brouns

februari 2014

Hoofdstuk 3: Tellen

3.3 opl Verdeel de driehoek in 4 kleinere deeldriehoeken, door de middelpunten van de zijden met elkaar te verbinden. Leg je vijf punten in de grote driehoek, dan liggen er minstens 2 in dezelfde deeldriehoek (ladenprincipe). De afstand tussen deze 2 is maximaal de lengte van de zijde van de deeldriehoek ($\frac{1}{2}$).

3.5 opl Enkelspel: kies 2 uit 6, dus $\binom{6}{2}$.
Dubbelspel: kies 2 uit 6, en 2 uit overblijvende 4. Volgorde van ploegen speelt geen rol, dus delen door 2. Dus $\dfrac{\binom{6}{2}\binom{4}{2}}{2} = ...$

3.6 opl Kies eerste punt: n manieren; kies tweede punt: $n-1$ manieren. Bepaalt samen eerste rechte.
Kies derde punt en vierde punt: $(n-2)(n-3)$ manieren.
Op hoeveel manieren had je die $2+2$ punten kunnen kiezen? Het eerste punt had je op 4 manieren kunnen kiezen, het tweede ligt dan vast (nl. via rechte); het derde punt had je op 2 manieren kunnen kiezen.
$\frac{1}{8}n(n-1)(n-2)(n-3)$

3.7 opl Aantal keuzes voor elk teken vermenigvuldigen: $26 \cdot 25 \cdot 24 \cdot 23 \ \cdot \ 26 \cdot 25 \cdot 24 \ \cdot \ 10 \cdot 9$.

3.8 opl

1. Hoeveel dergelijke getallen zijn er? 5^3
2. Wat is het volgnummer van 251, 333 en 454? $46e, 63e, 99e$
3. Welk getal staat op de 21e plaats? 151

3.9 opl $\binom{12}{6}\binom{6}{4}$
Voor tweede vraag: ga alle gevallen af, en tel bijhorende getallen op.

6	5	1
6	4	2
6	3	3
7	4	1
7	3	2
8	3	1
8	2	2
9	2	1
10	1	1

geeft

$$\binom{12}{6}\left[\binom{6}{5}+\binom{6}{4}+\binom{6}{3}\right]+\binom{12}{7}\left[\binom{5}{4}+\binom{5}{3}\right]+\binom{12}{8}\left[\binom{4}{3}+\binom{4}{2}\right]+\binom{12}{9}\binom{3}{2}+\binom{12}{10}\binom{2}{1}$$

3.11 opl Tussen 1500 en 2000 zitten er $1 \cdot 5 \cdot 8 \cdot 7$,
tussen 2000 en 4000 zitten er $2 \cdot 9 \cdot 8 \cdot 7$.
Samen: $(5 + 18) \cdot 8 \cdot 7 = 1288$.

3.12 opl Tel alle mogelijke (=12) sommen van 5 opeenvolgende getallen op. Je zal dan elk getal uit de cirkel 5 keer geteld hebben.
$5\sum_{i=1}^{12} i < 32 \cdot 12 \Leftrightarrow 13 \cdot 6 \cdot 5 < 32 \cdot 12 \Leftrightarrow 13 \cdot 5 < 32 \cdot 2$. Antwoord op de vraag: neen, dit is niet mogelijk.

3.13 opl Kies voor de rode rozenstruiken 4 van de 12 plaatsen, etc. Antwoord: $\binom{12}{4}\binom{8}{5}$.

3.14 opl

1. ANAGRAM $\frac{7!}{3!} = 840$.
2. BANANENBOOT $\frac{11!}{2!2!3!2!1!1!} = 831600$.
3. HOTTENTOTTENTENTENTENTOONSTELLING grapje...

Redenering voor woord van n letters: voor eerste plaats heb je n keuzes, voor tweede plaats nog $n - 1$,...
Eens het anagram gevormd is, zie je dat gelijke letters niet van elkaar onderscheiden kunnen worden, dus heb je $x!$ keer hetzelfde anagram gemaakt wat die bepaalde letter betreft.

3.15 opl Bij 0 hoort 0, bij 1 hoort 0 en 1, bij 2 hoort 0,1 en 2. Totale aantal (van 0 tot 6) is dus $1 + 2 + 3 + 4 + 5 + 6 + 7 = \frac{7 \cdot 8}{2} = 28$.

3.16 opl

1. Alle schapen in 1 kooi (die kooi valt op 4 manieren te kiezen)
   dus 5 wolven verdelen over 3 kooien (zoals frequentietabel), dat is nog $\overline{\binom{3}{5}} = \binom{7}{5}$.
   Vermenigvuldigen geeft $4 \cdot 21 = 84$.
2. Alle schapen in 2 kooien (waarbij minstens 1 schaap in elke kooi, anders zit je in geval 1):
   welke kooi? 2 uit 4 kiezen, is $\binom{4}{2}$.
   nog 8 schapen te verdelen over 2 kooien, is $\overline{\binom{2}{8}}$.
   nog 5 wolven te verdelen over 2 kooien, is $\overline{\binom{2}{5}}$.
   Samen: $\binom{4}{2}\binom{9}{8}\binom{6}{5} = 6 \cdot 9 \cdot 6 = 324$.

3. Alle schapen in 3 kooien waarbij geen enkele kooi leeg mag zijn (anders zitten we in andere gevallen).
   welke kooi? 3 uit 4 kiezen.
   in elke kooi minstens 1 schaap, dus nog 7 schapen over 3 kooien.
   alle wolven in 1 kooi: 1
   Samen: $4\binom{9}{7} = 4 \cdot 36 = 144$.
4. SOM: $84 + 324 + 144 = 552$.

3.19 opl Teken drie disjuncte verzamelingen, en geef aan hoeveel elementen er in elke verzameling zitten (indien al gekend). Daarna noteer je, volgens het principe van de dubbele telling, alle andere gegevens op verbindingslijnen tussen één element van de ene verzameling, en de andere verzameling. Werk gelijkheden uit naar de onbekenden. Oplossing: $q^2 + q + 1$.

Hoofdstuk 4: Voortbrengende functies

4.1 opl $1 - 2x + x^2$

4.2 opl

1. $(1 + x + x^2 + x^3)(1 + x + x^2 + x^3 + x^4 + x^5)$
2. $(1 + x + x^2 + x^3 + x^4)(1 + x + x^2 + x^3)(1 + x^2 + x^3 + x^5)$
3. $(1 + x^2 + x^4 + x^6 + \ldots)(1 + x^3 + x^6 + x^9 + \ldots)$
4. $(1 + x + x^2 + x^3)(1 + x + x^2 + x^3 + \ldots)$
5. $(x^4 + x^5 + x^6 + \ldots)(x^2 + x^3 + x^4 + \ldots)$

4.5 opl $a_k = k$ uit $M = 2xM - x^2M + x$

4.7 opl $\dfrac{10^n - 6^n}{2}$

4.8 opl $M = \dfrac{2 - 3x + 8x^2}{1 - x + 3x^2 - x^3}$

4.12 opl

1. $s_n = 3^n - n3^{n-1}$

Hoofdstuk 5: Diophantische vergelijkingen: lineair

5.2 opl $21 + k \cdot 210, k \in \boldsymbol{Z}$

5.3 opl $113 + k \cdot 180, k \in \boldsymbol{Z}$

5.4 opl 15, maar niet via stelling te vinden (eerder trial and error).

Hoofdstuk 6: Diophantische vergelijkingen: niet-lineair

6.1 opl 13

6.2 opl 307

6.3 opl 121

6.4 opl 9

6.7 opl Elk getal dat relatief priem is met 12 (en dus een mogelijke primitieve wortel is) heeft orde 2 (zie bijlage E), terwijl $\phi(12) = 4$.

6.8 opl

$\text{ord}_5 2$	$= 4$	primitieve wortel want $\phi(5) = 4$
$\text{ord}_{10} 3$	$= 4$	primitieve wortel want $\phi(10) = 4$
$\text{ord}_{13} 10$	$= 6$	geen primitieve wortel want $\phi 13 = 12$
$\text{ord}_{10} 7$	$= 4$	primitieve wortel want $\phi(10) = 4$

Hoofdstuk 7: Eindige velden

7.6 opl

1. $(1+x)^2(1+x+x^2)$
2. niet reduciebel
3. $(1+x)^3$
4. $(1+x)^4$
5. niet reduciebel
6. $(1+x+x^2)^2$
7. niet reduciebel
8. niet reduciebel

7.7 opl

1. $0 \quad 1 \quad \alpha \quad 1+\alpha$
2. $0 \quad 1 \quad \alpha \quad 1+\alpha \quad \alpha^2 \quad 1+\alpha^2 \quad \alpha+\alpha^2 \quad 1+\alpha+\alpha^2$
3. $0 \quad 1 \quad \alpha \quad 1+\alpha \quad \alpha^2 \quad 1+\alpha^2 \quad \alpha+\alpha^2 \quad 1+\alpha+\alpha^2$

7.9 opl Optellings- en vermenigvuldigingstabel voor het veld van 8 elementen, met $h(x) = 1+x+x^3$.

$+$	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
1	1	0	$1+\alpha$	α	$1+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$
α	α	$1+\alpha$	0	1	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$1+\alpha^2$
$1+\alpha$	$1+\alpha$	α	1	0	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2
α^2	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	0	1	α	$1+\alpha$
$1+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	1	0	$1+\alpha$	α
$\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$1+\alpha^2$	α	$1+\alpha$	0	1
$1+\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0								
1		1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
α		α	α^2	$\alpha+\alpha^2$	$1+\alpha$	1	$1+\alpha+\alpha^2$	$1+\alpha^2$
$1+\alpha$		$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$	α^2	1	α
α^2		α^2	$1+\alpha$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	α	$1+\alpha^2$	1
$1+\alpha^2$		$1+\alpha^2$	1	α^2	α	$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$
$\alpha+\alpha^2$		$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	1	$1+\alpha^2$	$1+\alpha$	α	α^2
$1+\alpha+\alpha^2$		$1+\alpha+\alpha^2$	$1+\alpha^2$	α	1	$\alpha+\alpha^2$	α^2	$1+\alpha$