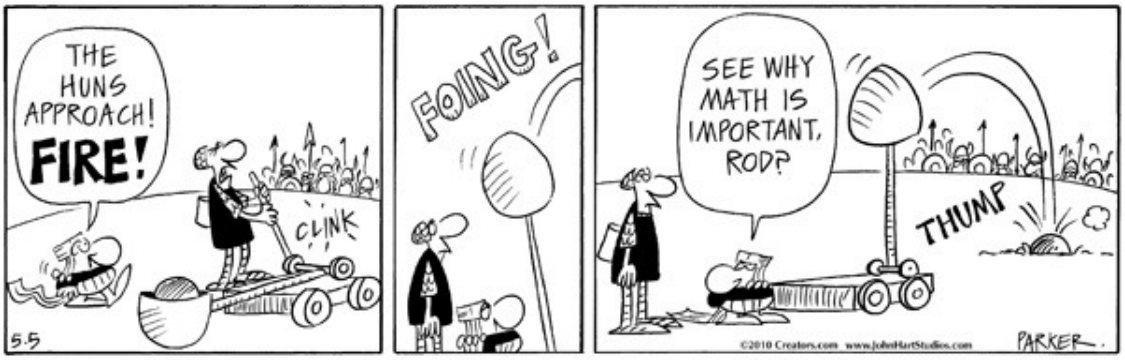
Inhoudsopgave



Hoofdstuk 1

Verzamelingen en relaties

1.1 De basisnotaties

Het begrip *verzameling* heb je zeker al in allerlei omstandigheden, binnen of buiten cursussen wiskunde, ontmoet. In de gewone spreektaal worden hiervoor heel wat synoniemen gebruikt. Volgende uitdrukkingen zijn je dus zeker niet vreemd: een *kudde* schapen, een *collectie* postzegels, een *regiment* soldaten, een *school* vissen, een *stapel* boeken, een *bende* schavuiten, een *stel* kookpotten, een *groep* studenten, ...

Al die uitdrukkingen wijzen erop dat sommige dingen samen beschouwd worden. Dit wordt dan aangeduid door het gebruik van woorden zoals kudde, collectie, regiment, ... verzameling. Binnen de wiskunde wordt het begrip *verzameling* gebruikt om te vertolken dat **verschillende** en **duidelijk gedefinieerde** dingen, die we dan *elementen* van de verzameling noemen, samen moeten worden beschouwd. Indien we de eis "verschillend" laten vallen, dan spreken we eerder van een *familie* van elementen, soms wordt in dat geval ook gesproken van een *multiverzameling*. De eis dat de elementen duidelijk gedefinieerd zijn is ook belangrijk. Zo kan je moeilijk spreken van de verzameling van de belangrijkste vakken in het eerste bachelorjaar informatica, omdat dit zeer subjectief is en dus niet duidelijk gedefinieerd. Je kan het wel hebben over de verzameling van al de vakken uit het eerste bachelorjaar, wat een eindige verzameling is. De elementen van een eindige verzameling kan je in principe dus expliciet opschrijven, maar indien de verzameling zeer veel elementen bezit is dit wat onhandig. Meer nog, voor een niet-eindige verzameling is dat gewoon niet mogelijk. In deze gevallen behelpen we ons met een omschrijving. Overigens, bij opsomming van de elementen in een verzameling speelt de volgorde geen rol. Een verzameling met één element wordt een *singleton* genoemd, terwijl een verzameling met twee elementen een *paar* genoemd wordt; niet te verwarren met een koppel (x, y) van twee elementen, ook wel een *geordend paar* genoemd.

De meeste notaties zijn wereldwijd vastgelegd en zijn je zeker bekend, zodat we hier niet lang moeten blijven bij stil staan. De volgende symbolenlijst zou dan ook moeten volstaan.

Notatie	Omschrijving
$\{a, b, c\}$	verzameling met als elementen a, b en c
$\{a, b, c, \dots\}$	verzameling met als elementen a, b en c, enz.
$\{x \mid \dots\}$	verzameling van alle elementen zodanig dat $\dots$
$\emptyset$	de ledige verzameling
$\in$	is element van (behoort tot)
$\notin$	is geen element van (behoort niet tot)
$\subseteq$	is deelverzameling van
$\not\subseteq$	is geen deelverzameling van
$A \cap B$	A doorsnede B
$A \cup B$	A unie B
$A \setminus B$	verschil van A en B (soms ook als $A - B$ genoteerd)

Opmerking

De bovenstaande lijst is zeker niet volledig, indien nodig zullen aanvullende notaties in de loop van de cursus worden ingevoerd.

Wat het begrip *deelverzameling* betreft moeten we misschien wat meer specifiek zijn. Indien we zeggen dat een verzameling A een deelverzameling is van B, dan bedoelen we dat elk element van A ook element is van B. De verzameling A kan dus ook samenvallen met B, vandaar dat we de notatie $A \subseteq B$ gebruiken. Soms wordt hiervoor ook de notatie $A \subset B$ gebruikt; indien men expliciet wil duidelijk maken dat A verschillend moet zijn van B, gebruikt men de notatie $A \subsetneq B$.

Overigens zullen we soms de symbolen uit de verzamelingenleer in zijn symmetrische vorm gebruiken zoals $A \ni a, A \supseteq B, \dots$

In de bovenstaande symbolenlijst hadden we het over de ledige verzameling $\emptyset$, het is de verzameling die geen enkel element bevat. Aan de andere kant van het spectrum, vooral van belang bij de theoretische behandeling van verzamelingenleer, zullen we het hebben over het *universum* of de *universele verzameling* die dan bestaat uit de verzameling van alle elementen die we op dat moment beschouwen. In tegenstelling tot de notatie voor de ledige verzameling bestaat hiervoor geen "universele" notatie, we zullen meestal Ω gebruiken.

Veronderstel dat A een deelverzameling is van een verzameling B, dan noemen we het *complement* van A, de verzameling van alle elementen van B die niet in A gelegen zijn. Elke verzameling A kan beschouwd wordt als deelverzameling van de universele verzameling Ω. Het complement van A is dan $A^c = \Omega \setminus A$. Het is eenvoudig na te gaan dat $(A^c)^c = A$; $A \cap A^c = \emptyset$ en $A \cup A^c = \Omega$.

Nu we de notaties min of meer hebben vastgelegd, kunnen we al een eerste reeks eigenschappen opsommen, die we hier in de vorm van een eerste stelling formuleren. Het bewijs is een eenvoudige oefening. Zoals meestal in de theorie van de verzamelingenleer, kunnen bewijzen ondersteund worden door het tekenen van Venn diagrammen (John Venn, 1834–1923).

Stelling 1.1.1. *Als A, B en C verzamelingen zijn, dan gelden de volgende eigenschappen.*

(1) **Commutatieve eigenschap**

   (a) $A \cap B = B \cap A$.

   (b) $A \cup B = B \cup A$.

(2) **Associatieve eigenschap**

   (a) $A \cap (B \cap C) = (A \cap B) \cap C$ *(en we noteren daarom $A \cap B \cap C$).*

   (b) $A \cup (B \cup C) = (A \cup B) \cup C$ *(en we noteren daarom $A \cup B \cup C$).*

(3) **Distributieve eigenschap**

   (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

   (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(4) **Wetten van De Morgan** *(August De Morgan (1806–1871))*

   (a) $(A \cup B)^c = A^c \cap B^c$.

   (b) $(A \cap B)^c = A^c \cup B^c$.

Het lezen waard

Het abstract beschrijven van verzamelingen kan soms tot eigenaardigheden leiden. Het meest bekend is de zogenaamde *Paradox van Russell* (Bertrand Russell, 1872–1970).

> Veronderstel dat R de verzameling is van alle verzamelingen die geen element zijn van zichzelf. Dan is R noch een element van zichzelf noch geen element van zichzelf.

Met de notaties die we tot hiertoe hebben gezien, betekent dit dus dat als $R = \{x \mid x \notin x\}$ dan is $R \in R$ gelijkwaardig met $R \notin R$.

Een paradox die zijn eigen leven is gaan leiden. Hoe komen we hier uit?

1.2 Relaties

1.2.1 Basisdefinities

Het *cartesisch product* van twee verzamelingen A en B, ook nog *productverzameling* genoemd, is de verzameling

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Het is dus duidelijk dat voor twee verschillende verzamelingen A en B geldt dat $A \times B \neq B \times A$. Meer algemeen wordt het cartesisch product van k verzamelingen $A_1, A_2, \ldots, A_k$ gedefinieerd als

$$A_1 \times A_2 \times \cdots \times A_k = \{(a_1, a_2, \ldots, a_k) \mid a_i \in A_i, i = 1, 2, \ldots, k\}.$$

De elementen van deze verzamelingen worden *geordende k-tallen* genoemd. Indien $A_i = A$ voor alle $i \in \{1, 2, \ldots, k\}$ dan noteren we het cartesisch product als A^k. Het is duidelijk dat de term "cartesisch product" afkomstig is van het begrip "cartesisch assenstelsel" waarbij bijvoorbeeld voor elk punt van de driedimensionale ruimte met coördinaten in de verzameling $\mathbb{R}$ van de reële getallen, elk punt uniek bepaald is door zijn coördinaat (x, y, z). Op zijn beurt verwijst cartesisch naar de Franse filosoof René Descartes (1596-1650), die in zijn werk *La géométrie*, de toepassing beschrijft van de algebra in de studie van de meetkunde, hetgeen dan geleid heeft tot de term cartesisch of cartesiaans assenstelsel.

Een *relatie* van een verzameling A naar een verzameling B is een deelverzameling van de productverzameling $A \times B$. Het is dus een verzameling $\mathcal{R}$ van koppels met eerste element (begin van het koppel) in A en tweede element in B (einde van het koppel). We noemen A de *beginverzameling* en B de *eindverzameling*. Als $(a, b) \in \mathcal{R}$, dan wordt b een *beeld* genoemd van a onder de relatie $\mathcal{R}$, en soms wordt dit genoteerd als $a\mathcal{R}b$ (denk bijvoorbeeld aan $a \leq b$), maar ook als $b = \mathcal{R}(a)$, al wordt deze laatste notatie bijna uitsluitend gebruikt voor functies (zie paragraaf 1.2.2). Een relatie kan voorgesteld worden door middel van pijlen van de verzameling A naar de verzameling B, of kan voorgesteld worden als punten in het vlak met coördinaatassen A en B. Indien $A = B$ dan spreken we eerder van een relatie in A.

Voorbeeld

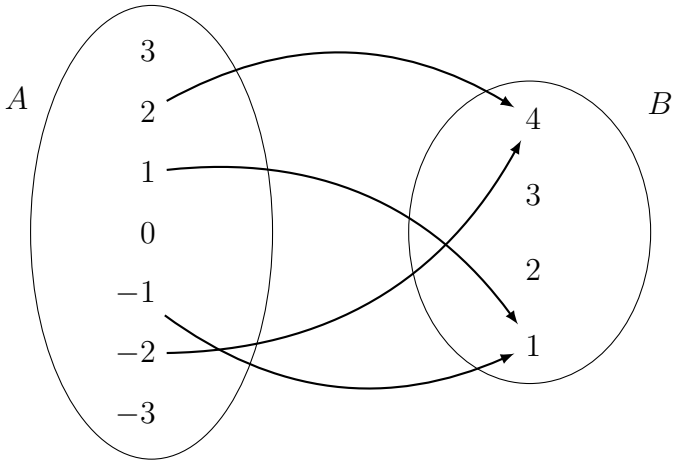
Beschouw de verzamelingen $A = \{-3, -2, -1, 0, 1, 2, 3\}$, $B = \{1, 2, 3, 4\}$, en de relatie

$$\mathcal{R} = \{(a, b) \in A \times B \mid a^2 = b\}.$$

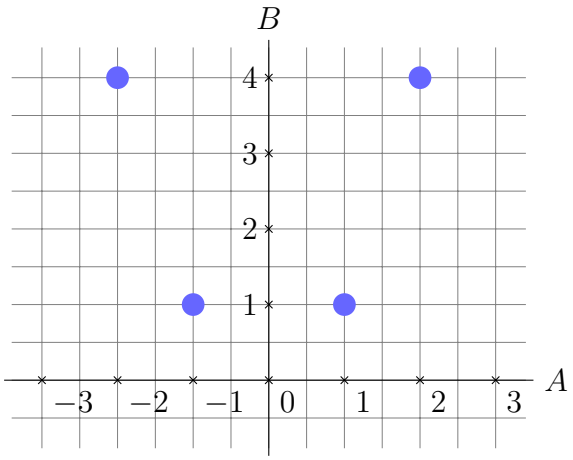
Dan is

$$\mathcal{R} = \{(-2,4),(2,4),(-1,1),(1,1)\}\,.$$

Als we $\mathcal{R}$ voorstellen door middel van pijlen van A naar B, krijgen we de volgende figuur.



De coördinaatassen-voorstelling van $\mathcal{R}$ ziet er als volgt uit.



Als $\mathcal{R} \subseteq A \times B$ een relatie is, dan is per definitie de *omgekeerde* of *inverse relatie* de verzameling $\mathcal{R}^{-1}$ van de omgekeerde koppels, d.w.z.

$$\mathcal{R}^{-1} = \{(b,a) \mid (a,b) \in \mathcal{R}\}\,,$$

en is dus een deelverzameling van $B \times A$.

Als (a,b) en (b,c) twee koppels zijn, die dus het kenmerk vertonen dat het einde van het eerste koppel precies het begin is van het tweede koppel,

dan zeggen we dat het koppel (b, c) volgt op het koppel (a, b) of nog, dat de koppels (a, b) en (b, c) opeenvolgende koppels zijn. Het koppel (a, c) gevormd door het begin van het eerste koppel en het einde van het tweede koppel, wordt de *samenstelling* van de twee opeenvolgende koppels genoemd.

Als $\mathcal{R}_1$ een relatie is van een verzameling A naar een verzameling B en $\mathcal{R}_2$ een relatie is van een verzameling B naar een verzameling C, dan wordt de verzameling van al de samengestelde koppels de *samenstelling* of *samengestelde relatie* van $\mathcal{R}_1$ en $\mathcal{R}_2$ genoemd, het is een relatie van A naar C en wordt genoteerd als $\mathcal{R}_2 \circ \mathcal{R}_1$ (lees: $\mathcal{R}_2$ na $\mathcal{R}_1$).

Het is duidelijk dat de samenstelling van relaties (indien gedefinieerd) associatief is $(\mathcal{R}_3 \circ (\mathcal{R}_2 \circ \mathcal{R}_1) = (\mathcal{R}_3 \circ \mathcal{R}_2) \circ \mathcal{R}_1)$ maar dat de commutatieve eigenschap niet geldt $(\mathcal{R}_1 \circ \mathcal{R}_2 \neq \mathcal{R}_2 \circ \mathcal{R}_1)$.

Verder is duidelijk dat de omgekeerde van een samengestelde relatie de samenstelling is van de omgekeerde relaties maar dan wel in de omgekeerde volgorde:

$$(\mathcal{R}_2 \circ \mathcal{R}_1)^{-1} = \mathcal{R}_1^{-1} \circ \mathcal{R}_2^{-1}.$$

Opmerking

Wat de notatie voor waarden van een relatie betreft, wordt ook wel de zogenaamde exponentiële notatie gebruikt; opnieuw geldt dat een dergelijke notatie bijna uitsluitend voor functies wordt toegepast. Als $(a, b) \in \mathcal{R}_1$ dan schrijven we $b = a^{\mathcal{R}_1}$. Dit heeft dan wel als gevolg dat wat de samenstelling betreft, voor $(a, b) \in \mathcal{R}_1$ en $(b, c) \in \mathcal{R}_2$, we de samenstelling anders zullen noteren, namelijk als $\mathcal{R}_1\mathcal{R}_2$, wat dan weer zinvol is, want $a^{\mathcal{R}_1\mathcal{R}_2} = (a^{\mathcal{R}_1})^{\mathcal{R}_2} = b^{\mathcal{R}_2} = c$.

1.2.2 Bijzondere relaties

Bij de definitie van een relatie van een verzameling A naar een verzameling B hebben we geen restricties gelegd op het bestaan van de beelden; een element van A kan meerdere, één of geen enkel beeld hebben. Naargelang het aantal beelden dat de elementen van A hebben, willen we nu een onderscheid maken tussen bepaalde soorten relaties van A naar B.

- Een *functie* van A naar B is een relatie van A naar B waarbij elk element van A hoogstens één beeld heeft. Anders gezegd, in de pijlenvoorstelling van een functie vertrekt in elk element van A ten hoogste één pijl.

- Een *afbeelding* van A naar B is een relatie van A naar B waarbij elk element van A juist één beeld heeft. Opgelet, een element van B kan

beeld zijn van meerdere verschillende elementen van A. Anders gezegd, in de pijlenvoorstelling van een afbeelding vertrekt in elk element van A juist één pijl. Elke afbeelding is dus een functie, maar niet omgekeerd. Overigens is het duidelijk dat het omgekeerde van een afbeelding (in het bijzonder van een functie) niet noodzakelijk een afbeelding is. Indien $A = B$ dan spreken we soms van een *transformatie van* A in plaats van afbeelding van A naar A.

Opmerking

We kunnen een eerder filosofische discussie opstarten rond de verschillen tussen een functie en een afbeelding, in het bijzonder wat de benaming van de beginverzameling A betreft. In de theorie van de functies wordt de deelverzameling van A waar de pijlen vertrekken, en dus de functie gedefinieerd is, meestal de *definitieverzameling* of het *definitiegebied* genoemd. Een afbeelding is dan in deze context een functie waarbij het definitiegebied samenvalt met de beginverzameling. Een analoog onderscheid kan overigens gemaakt worden naar de beeldenverzameling toe, die dus een (al of niet eigenlijke) deelverzameling is van de eindverzameling B. In de analyse wordt eerder gesproken over A-B-functies. Anderzijds wordt daar ook gesproken over *reële functies*, waarbij eigenlijk alleen bedoeld wordt dat de eindverzameling een deelverzameling is van de verzameling $\mathbb{R}$ van de reële getallen.

Ook de begrippen *domein* voor beginverzameling en *codomein* voor eindverzameling komen voor, maar om de verwarring nog groter te maken, zal in vele handboeken analyse (en ook in de cursus analyse) de term *domein* gebruikt worden als een synoniem voor *definitiegebied* eerder dan voor de term *beginverzameling*. De context zal moeten duidelijk maken wat bedoeld wordt.

- Een relatie met beginverzameling A en eindverzameling B wordt een *injectieve* relatie van A *in* B genoemd als elk element van de eindverzameling beeld is van hoogstens één element van de beginverzameling. Met andere woorden in de pijlenvoorstelling van een injectieve relatie komt in elk element van B hoogstens één pijl toe. Indien de relatie van A naar B een afbeelding is, dan spreken we kortweg van een *injectie* van A in B, wat voor de pijlenvoorstelling betekent dat er juist één pijl vertrekt uit A en hoogstens één pijl toekomt in B. Soms worden injectieve functies ook wel kortweg injecties genoemd.

- Een relatie met beginverzameling A en eindverzameling B wordt een *surjectieve* relatie van A *op* B genoemd, als elk element van de eindverzameling beeld is van minstens één element van de beginverzameling.

Met andere woorden in de pijlenvoorstelling van een surjectieve relatie komt in elk element van B minstens één pijl toe. Indien de relatie van A naar B een afbeelding is, dan spreken we kortweg van een *surjectie* van A op B, wat voor de pijlenvoorstelling betekent dat er juist één pijl vertrekt uit A en minstens één pijl toekomt in B. Ook surjectieve functies worden soms kortweg surjecties genoemd.

- Een *bijectie* van A op B is een afbeelding die zowel een injectie is als een surjectie. In de pijlenvoorstelling van een bijectie betekent dit dat in elk element van A juist één pijl vertrekt en dat in elk element van B juist één pijl toekomt. Een bijectie van A op B is dus een afbeelding van A in B waarvan de omgekeerde eveneens een afbeelding is (van B naar A). Wanneer er een bijectie bestaat van A naar B (en dus ook van B in A) dan zeggen we dat beide verzamelingen *gelijkmachtig* zijn. Voor eindige verzamelingen betekent dit eigenlijk dat deze verzamelingen evenveel elementen bezitten.

- Een bijectie van een verzameling A op zichzelf wordt een *permutatie* genoemd. Voor een eindige verzameling correspondeert dit begrip inderdaad met ons intuïtief begrip van permuteren van een aantal elementen, in de betekenis van verwisselen van volgorde van deze elementen, hierover meer in het deel combinatieleer.

1.2.3 Equivalentierelaties

In deze sectie zullen we het steeds hebben over relaties in een verzameling A (dus met zelfde begin- en eindverzameling).

- Een relatie $\mathcal{R} \subseteq A^2$ wordt *reflexief* genoemd, als voor elk element x van A, het *identieke koppel* (x, x) tot $\mathcal{R}$ behoort. Indien geen enkel identiek koppel tot $\mathcal{R}$ behoort, dan noemen we $\mathcal{R}$ een *antireflexieve* relatie, niet te verwarren met een *niet-reflexieve* relatie, wat een relatie is die niet alle identieke koppels van A bevat. In de pijlenvoorstelling van een relatie wordt een identiek koppel voorgesteld door een lus (zonder pijl). In een reflexieve relatie komen in de pijlenvoorstelling alle lussen voor. In een niet-reflexieve relatie komen sommige lussen niet voor. In een antireflexieve relatie komen nooit lussen voor.

- Een relatie $\mathcal{R} \subseteq A^2$ wordt *symmetrisch* genoemd als voor elke twee elementen x en y van A zodanig dat $(x, y) \in \mathcal{R}$ volgt dat ook $(y, x) \in \mathcal{R}$. De relatie wordt *antisymmetrisch* genoemd indien voor elk niet-identiek koppel dat tot $\mathcal{R}$ behoort, het omgekeerde koppel niet tot $\mathcal{R}$ behoort.

Of nog, indien zowel (x, y) als (y, x) tot $\mathcal{R}$ behoren dan moet $x = y$. Ook hier mag niet verward worden met het begrip *niet-symmetrische* relatie.

- Een relatie $\mathcal{R} \subseteq A^2$ wordt *transitief* genoemd als de samenstelling van twee opeenvolgende koppels van die relatie altijd tot de relatie behoort. Met andere woorden, als voor drie elementen x, y, z van A geldt dat zowel (x, y) als (y, z) tot een transitieve relatie $\mathcal{R}$ behoren, dan zal ook (x, z) tot $\mathcal{R}$ behoren.

Met de bovenstaande begrippen kunnen we nu de definitie geven van een *equivalentierelatie* $\mathcal{R} \subseteq A^2$. Het is een relatie die tegelijkertijd **reflexief, symmetrisch en transitief** is. Als $(a, b) \in \mathcal{R}$, dan noemen we a *equivalent met* b en we noteren dit dan als $a \equiv b$. Eenvoudige voorbeelden van equivalentierelaties zijn:

- "zelfde leeftijd hebben"(in bijvoorbeeld de verzameling van alle studenten van het eerste bachelorjaar informatica);
- "parallellisme van rechten" (in bijvoorbeeld het Euclidisch vlak);
- "zelfde rest bezitten na deling door een natuurlijk getal m (in de verzameling van de gehele getallen)".

Alle elementen van A die equivalent zijn met $a \in A$, vormen een deelverzameling van onderling equivalente elementen van A; dergelijke deelverzameling wordt een *equivalentieklasse* van de equivalentierelatie $\mathcal{R}$ genoemd. We zullen voorlopig de equivalentieklasse die het element a bevat noteren door $[a]$ en noemen a een *representant* van deze klasse. Merk overigens op dat als $b \equiv a$, dan uiteraard $[b] = [a]$, of nog, elk element van $[a]$ kan als representant van deze klasse genomen worden. Uit de bovenstaande definitie volgt onmiddellijk dat geen enkele equivalentieklasse ledig kan zijn, dat twee verschillende equivalentieklassen altijd een ledige doorsnede hebben en dat bovendien de unie van alle equivalentieklassen de volledige verzameling A is. In de verzamelingenleer wordt elke verzameling van deelverzamelingen van A die de eigenschap bezit dat geen enkele deelverzameling ledig is en zodanig dat elk element van A tot juist één dergelijke deelverzameling behoort, een *partitie* genoemd van A. Het is nu duidelijk dat elke equivalentierelatie in een verzameling A aanleiding geeft tot een partitie van A, maar ook omgekeerd dat elke partitie van A aanleiding geeft tot een equivalentierelatie van A. Met andere woorden, de begrippen *equivalentierelatie* en *partitie* zijn "equivalente" of gelijkwaardige begrippen.

Hoofdstuk

2 Getallen tellen

2.1 De gehele getallen

2.1.1 Inleiding

Van Leopold Kronecker is geweten dat hij eens uitriep:

> *God schiep de natuurlijke getallen en de rest is het werk van de mens.*

Sommige computerfreaks hebben deze bekende uitspraak geparafraseerd door te stellen

> *God schiep de getallen 0 en 1, en de rest is het werk van de computer.*

Het is zonder meer duidelijk dat de natuurlijke getallen ons van kindsaf zijn ingelepeld, allemaal hebben wij moeten leren *tellen*, meestal op de vingers, en dan klonk het $1, 2, 3, 4, 5, \ldots$. De naam *natuurlijke getallen* is dan ook niet verkeerd gekozen. Alleen, wij willen meer doen met deze getallen. Wij willen ze bijvoorbeeld optellen, wij willen ze ordenen en nog meer dergelijke zaken. Strikt gesproken moeten wij hier een definitie geven van *tellen* en *optellen*; het is echter niet onze bedoeling om deze cursus te starten van uit het niets, en wij nemen derhalve aan dat deze begrippen *primitieve* begrippen zijn.

Wij merken terloops op dat wij ervan uitgaan dat de begrippen uit de verzamelingenleer en hun notaties voldoende gekend zijn. Wij zullen deze notaties hier steeds ongestoord gebruiken.

Terug naar de *verzameling van de natuurlijke getallen*. Indien wij enige structuur op deze verzameling willen leggen, dan is het al vlug duidelijk dat wij een notatie moeten hebben voor *niets*. Dit is de aanleiding geweest om een extra element, genoteerd door 0, bij te voegen. Men kan nu discussieren over het feit of 0 al dan niet een natuurlijk getal is. Internationaal zijn hierover geen afspraken gemaakt. Voor de ene is het getal (of moeten wij zeggen symbool) 0 geen natuurlijk getal, voor anderen wel. Indien wij

het, zoals in dit hoofdstuk, over allerhande telproblemen hebben, is het meer logisch om te starten van het getal 1. Wij gebruiken de volgende notaties.

$$\begin{aligned}\mathbb{N} &= \{0, 1, 2, 3, \ldots\} \\ \mathbb{N}^* &= \{1, 2, 3, \ldots\} = \mathbb{N} \setminus \{0\}.\end{aligned}$$

Misschien ben je gewoon om de notatie $\mathbb{N}_0$ te gebruiken voor $\mathbb{N}^*$, maar dit doen we liever niet, omdat dit een wat onlogische notatie is.

Eens we kunnen optellen, willen wij ook de inverse bewerking (die wij dus *aftrekken* noemen) uitvoeren. Uiteraard willen wij binnen onze verzameling van de natuurlijke getallen blijven, maar dit kan echter niet altijd. Wij zijn dus verplicht de verzameling van de natuurlijke getallen uit te breiden met nieuwe getallen, de zogenaamde *negatieve gehele getallen*. Voegen wij hier de natuurlijke getallen bij, die we dus ook de *niet-negatieve gehele getallen* kunnen noemen, dan ontstaat de verzameling van de gehele getallen

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

Alhoewel de notatie $\mathbb{Z}$ voor de verzameling van de gehele getallen een internationale standaardnotatie is (komt van het Duits *Zahl*), geldt dit niet voor de notatie en benaming van de verzameling van de negatieve gehele getallen en andere deelverzamelingen van $\mathbb{Z}$. Wij noteren (bewust van enige inconsequenties)

$$\begin{aligned}\mathbb{Z}^- = \mathbb{Z}_{\leq 0} &= \{0, -1, -2, -3, -4, \ldots\} \\ \mathbb{Z}^+ = \mathbb{Z}_{\geq 0} &= \{0, 1, 2, 3, 4, \ldots\} = \mathbb{N} \\ \mathbb{Z}^{+*} = \mathbb{Z}_{>0} &= \{1, 2, 3, 4, \ldots\} = \mathbb{N}^* \\ \mathbb{Z}^{-*} = \mathbb{Z}_{<0} &= \{-1, -2, -3, -4, \ldots\}.\end{aligned}$$

Merk op dat 0 noch positief noch negatief is, de benaming *strikt positieve getallen* voor $\mathbb{N}^*$ is dus niet zinvol, we spreken daarom liever van de natuurlijke getallen zonder 0 of van de positieve gehele getallen. Om dezelfde reden noemen we $\mathbb{Z}^-$ de verzameling van de *negatieve gehele getallen samen met 0* maar het is korter om te spreken over de *niet-positieve gehele getallen*.

We voeren tenslotte nog een laatste notatie in (die weliswaar terug niet standaard is):

$$\mathbb{N}[a, b] = \{a, a + 1, a + 2, \ldots, b - 1, b\} \subseteq \mathbb{N}.$$

Een analoge notatie zal gebruikt worden voor deelverzamelingen van de andere getallenverzamelingen.

De gehele getallen werden ingevoerd om de inverse bewerking van de optelling steeds mogelijk te maken. Er is echter nog een tweede bewerking die ons van kindsbeen werd bijgebracht, met name de vermenigvuldiging. Indien wij hiervan de inverse bewerking willen uitvoeren, dan blijkt al vlug dat wij terug nieuwe getallen moeten invoeren, met name de (eigenlijke) *breuken*. Samen met de gehele getallen vormen zij de verzameling van de *rationale getallen*, die door $\mathbb{Q}$ voorgesteld wordt. Deze verzameling wordt dan nog uitgebreid met de zogenaamde *irrationale getallen*, om dan de verzameling $\mathbb{R}$ van de *reële getallen* te vormen. Deze verzameling wordt dan op zijn beurt nog uitgebreid tot de verzameling $\mathbb{C}$ van de *complexe getallen* $\mathbb{C}$. De structuur van deze verzamelingen ten opzichte van de "natuurlijke" bewerkingen, optelling (en aftrekking) en vermenigvuldiging (en deling) komt in het secundair onderwijs voldoende aan bod. Wij zullen op hun structuur terug komen in het hoofdstuk over velden.

2.1.2 De optelling en de vermenigvuldiging

Wat echter de gehele getallen betreft, zouden wij kunnen stellen dat de optelling en de vermenigvuldiging van gehele getallen a en b, bewerkingen zijn die aan de volgende wetmatigheden of *axioma's* voldoen.

(A1) Voor alle $a, b \in \mathbb{Z}$ geldt $a + b \in \mathbb{Z}$ en $ab \in \mathbb{Z}$. De verzameling van de gehele getallen is met andere woorden *gesloten* voor de bewerkingen optelling en vermenigvuldiging, of nog de vermenigvuldiging en de optelling zijn *inwendige bewerkingen*.

(A2) Voor alle $a, b \in \mathbb{Z}$ geldt $a + b = b + a$ en $ab = ba$. De bewerkingen optelling en vermenigvuldiging zijn *commutatieve* of *abelse* bewerkingen.

(A3) Voor alle $a, b, c \in \mathbb{Z}$ geldt $(a + b) + c = a + (b + c)$ en $(ab)c = a(bc)$. De bewerkingen optelling en vermenigvuldiging zijn *associatieve* bewerkingen.

(A4) Voor alle $a \in \mathbb{Z}$ geldt $a + 0 = a$ en $a \cdot 1 = a$. Het geheel getal 0 is het *neutraal element voor de optelling*; het geheel getal 1 is het *neutraal element voor de vermenigvuldiging*.

(A5) Voor alle $a, b, c \in \mathbb{Z}$ geldt $a(b + c) = ab + ac$. De (linkse) *distributiviteitsregel* (en wegens **(A2)** ook de rechtse) van de vermenigvuldiging t.o.v. de optelling geldt.

(A6) Voor alle $a \in \mathbb{Z}$ bestaat er een element $-a \in \mathbb{Z}$ zodat $a + (-a) = 0$. Elk geheel getal bezit een *invers* geheel getal.

(A7) Als $ab = ac$ en $a \neq 0$, dan is $b = c$. De *linkse schrappingswet* (en wegens **(A2)** ook de rechtse) geldt voor de vermenigvuldiging.

Al deze axioma's worden door ons als natuurlijke wetmatigheden aanvaard. De meeste rekenregels die wij dagelijks gebruiken, kunnen uit deze axioma's worden afgeleid. Zo kan bijvoorbeeld de *aftrekking* van 2 gehele getallen a en b *gedefinieerd* worden als $a - b := a + (-b)$.

Oefeningen

1. Zoals gebruikelijk noteren wij xx met x^2. Bewijs op basis van de gegeven axioma's, dat voor elke 2 gegeven gehele getallen a en b er een geheel getal c bestaat zodanig dat $(a + b)c = a^2 - b^2$.

2. Bewijs op basis van de gegeven axioma's dat het getal 0 het enige neutraal element is voor de optelling en dat elk geheel getal een uniek invers geheel getal bezit.

2.1.3 De ordening van de gehele getallen

De natuurlijke *ordening* (of *orde*) "kleiner dan of gelijk aan" ($\leq$) van de gehele getallen is op zijn minst even belangrijk als de bovenstaande rekenregels. Deze ordening is opnieuw, als gevolg van ons intuïtief begrip van tellen, een natuurlijke wetmatigheid voor ons geworden.

Een relatie $\mathcal{R}$ wordt een *orderelatie* of *ordening* genoemd, als ze reflexief, anti-symmetrisch en transitief is. We drukken deze drie voorwaarden expliciet als volgt uit voor de relatie $\mathcal{R} = \leq$.

(A8) $\leq$ is *reflexief*: Voor alle $a \in \mathbb{Z}$ geldt $a \leq a$.

(A9) $\leq$ is *anti-symmetrisch*: Voor alle $a, b \in \mathbb{Z}$ geldt: als $a \leq b$ en $b \leq a$, dan is $a = b$.

(A10) $\leq$ is *transitief*: Voor alle $a, b, c \in \mathbb{Z}$ geldt: als $a \leq b$ en $b \leq c$, dan is ook $a \leq c$.

Indien elke 2 verschillende elementen van een verzameling met elkaar vergeleken kunnen worden d.m.v. een orderelatie, dan noemt men dit een *totale orderelatie* of *totale ordening*.

(A11) $\leq$ is *totaal*: Voor alle $a, b \in \mathbb{Z}$ geldt $a \leq b$ of $b \leq a$.

Een orderelatie die niet totaal is, wordt een *partiële orderelatie* genoemd. De relatie a deelt b ($a \mid b$) is een voorbeeld van een partiële orderelatie; in deze relatie kunnen niet elke twee verschillende elementen met elkaar vergeleken worden. (Zo is bijvoorbeeld noch $2 \mid 3$ noch $3 \mid 2$.)

Merk terloops op dat $<$ en $>$ zogenaamde *strikt-orderelaties* zijn; deze relaties zijn *transitief* en *anti-reflexief* (niet te verwarren met *niet-reflexief*).

Ten slotte hebben we nog twee axioma's die de relatie $\leq$ in verband brengen met de bewerkingen op de gehele getallen.

(A12) Voor alle $a, b, c \in \mathbb{Z}$ geldt: als $a \leq b$, dan ook $a + c \leq b + c$.

(A13) Voor alle $a, b, c \in \mathbb{Z}$ geldt: als $a \leq b$ en $c \geq 0$, dan ook $ac \leq bc$.

Oefeningen

1. Veronderstel dat $a \leq b$. Gebruik de bovenstaande axioma's om te bewijzen dat $-b \leq -a$, of algemeen, bewijs dat uit $a \leq b$ en $c \leq 0$ volgt dat $bc \leq ac$.

2. Bewijs dat $0 \leq x^2$ voor elk geheel getal x, en bewijs hieruit dat $0 \leq 1$.

3. Bewijs dat $n \leq n + 1$ voor elk geheel getal n.

2.1.4 Het axioma van de goede ordening

Alhoewel wij nu op het eerste gezicht alle eigenschappen van $\mathbb{Z}$ kunnen afleiden van de bovenstaande 12 axioma's, moeten wij echter nog een belangrijk axioma toevoegen. Inderdaad, noem X een willekeurige deelverzameling van $\mathbb{Z}$, dan zeggen we dat het geheel getal b een *benedengrens* is voor X als $b \leq x$, $\forall x \in X$. Een benedengrens voor een verzameling X, die eveneens tot deze verzameling behoort, wordt *het kleinste element* van X genoemd. Het laatste axioma dat wij nu moeten toevoegen luidt:

(A14) Als X een deelverzameling is van $\mathbb{Z}$, verschillend van de ledige deelverzameling, die een benedengrens heeft, dan bezit zij een kleinste element.

Dit axioma is beter gekend onder de naam *axioma van de goede ordening* of het *well-ordening axioma*. Dat dit een eigenschap is die geldt voor de gehele getallen moge duidelijk zijn, maar deze eigenschap geldt niet meer in de verzameling van de rationale getallen. Zo zal bijvoorbeeld de verzameling $X = \{(n + 1)/n \mid n \in \mathbb{Z}, n \geq 2\}$ wel degelijk een benedengrens hebben (bijvoorbeeld 1), maar zij bezit geen kleinste element, wij kunnen inderdaad steeds een breuk vinden die kleiner is dan een gekozen breuk, en zo dichter

het getal 1 benaderen, maar nooit is het quotiënt $(n+1)/n$ $(n \geq 2)$ gelijk aan 1. Dus $1 \notin X$.

Een beetje niet-wiskundig kan men stellen, dat er gaten tussen 2 opeenvolgende gehele getallen voorkomen, dit drukt men uit door te zeggen dat $\mathbb{Z}$ een *discrete verzameling* is, in tegenstelling tot bijvoorbeeld $\mathbb{R}$ die een *dichte verzameling* is. Een groot aantal eigenschappen en rekenregels uit de analyse maken gebruik van het feit dat men over dichte verzamelingen werkt. Men zou daarom kunnen stellen dat *discrete wiskunde* de tegenpool is van de *calculus*.

Oefeningen

1. Een deelverzameling Y van $\mathbb{Z}$ heeft een *bovengrens* c als $c \geq y$, $\forall y \in Y$. Indien een bovengrens eveneens tot Y behoort, wordt het een grootste element van Y genoemd. Gebruik axioma **(A14)** om aan te tonen dat indien Y niet ledig is en een bovengrens bezit, het eveneens een grootste element bezit.

2. De natuurlijke getallen n, $1 \leq n \leq 25$, worden in een vierkant rooster van 5 rijen en 5 kolommen op een willekeurige manier geplaatst (elk getal komt slechts één keer voor). Van elke rij wordt het grootste element gekozen, en s wordt het kleinste onder die grootste elementen genoemd. Analoog wordt het kleinste element van elke kolom genomen, en weze t het grootste onder hen. Bewijs dat $s \geq t$. Geef een voorbeeld waarvoor $s \neq t$.

2.2 Recursieve definities

Als X een deelverzameling is van $\mathbb{N}$ of van $\mathbb{N}^*$, dan heeft het automatisch een benedengrens. Bijgevolg zal het axioma van de goede ordening hier de volgende vorm aannemen:

(A14) Als X een niet-ledige deelverzameling is van $\mathbb{N}$ of $\mathbb{N}^*$, dan bezit X een kleinste element.

Dit axioma van de goede ordening geeft ons de gelegenheid om een veel gebruikte procedure te rechtvaardigen. We komen geregeld functies tegen zoals

$$\begin{array}{rccc} u: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & 3n+2 \end{array}$$

Het is dan geen probleem om voor een specifieke waarde van n het getal $u(n)$ uit te rekenen. Een andere methode om een functie te definiëren is de *recursie* of *recursieve definitie*. In dit geval wordt de functie u met behulp van een uitdrukking geformuleerd die zelf u weer bevat (een dergelijke uitdrukking wordt een *recurrente betrekking* genoemd), zoals in het volgende voorbeeld.

$$u(1) = 1, \quad u(2) = 2, \quad u(n) = u(n-1) + u(n-2) \ \ (n \geq 3).$$

Wij hebben dan geen enkel probleem om de *opeenvolgende* waarden van $u(n)$ te berekenen. Het is de gewoonte de waarden $u(n)$ als u_n te noteren. De rij van de waarden, geordend volgens stijgende waarden van n, wordt genoteerd als $(u_n)_{n\in\mathbb{N}}$.

Alhoewel dit op het eerste gezicht triviaal lijkt, hebben wij het axioma van de goede ordening nodig om aan te tonen dat er voor elke n een unieke u_n is gedefinieerd. Inderdaad, veronderstel dat er ten minste één natuurlijk getal n bestaat waarvoor u_n niet uniek bepaald is. Als gevolg van het axioma van de goede ordening bestaat er dan een kleinste positief getal m zodanig dat u_m niet bepaald is. Aangezien u_1 en u_2 expliciet gegeven zijn, moet $m \geq 3$ en zal dus $u_m = u_{m-1} + u_{m-2}$. Wegens de definitie van m echter, zijn u_{m-1} en u_{m-2} uniek bepaald, zodat de som van deze getallen, met name het getal u_m uniek bepaald is, hetgeen tegen de veronderstelling is. Bijgevolg is elke u_n uniek gedefinieerd.

Een ander voorbeeld van een recursieve definitie, is de volgende

$$s_1 = 1, \quad s_n = s_{n-1} + (2n-1) \ \ (n \geq 2).$$

Dergelijke recursieve definitie kan verkort voorgesteld worden door

$$s_n = \sum_{i=1}^{n} (2i-1),$$

en is dus, als gevolg van het axioma van de goede ordening, een geldige definitie in $\mathbb{N}^*$. Merk echter op dat voor de effectieve berekening, bijvoorbeeld met de computer, de recursieve definitie $s_1 = 1,\ s_n = s_{n-1} + (2n-1)$ $(n \geq 2)$ gebruikt moet worden.

Een ander voorbeeld van verkorte schrijfwijze van een recursieve definitie vinden wij bij producten. Zo weten wij dat

$$n! := \prod_{i=1}^{n} i,$$

maar om het effectief uit te rekenen (en aan de computer duidelijk te maken), moet de volgende recursieve definitie gebruikt worden:

$$1! = 1, \quad n! = n \cdot (n-1)! \ \ (n \geq 2).$$

Soms zullen we ook de notatie $a_1 + \cdots + a_n$ gebruiken i.p.v. $\sum_{i=1}^{n} a_i$ en $a_1 \cdots a_n$ voor $\prod_{i=1}^{n} a_i$.

Oefeningen

1. Geef een recursieve definitie van $u_n = 2^n$ voor alle $n \geq 1$.

2. Schrijf een expliciete formule voor de uitdrukkingen u_n die als volgt recursief gedefinieerd worden.

   (a) $u_1 = 1, \quad u_n = u_{n-1} + 3 \ \ (n \geq 2)$.

   (b) $u_1 = 1, \quad u_n = n^2 u_{n-1} \ \ (n \geq 2)$.

2.3 Het inductieprincipe

Veronderstel dat er gevraagd wordt om de volgende formule te bewijzen

$$\sum_{i=1}^{n} (2i - 1) = n^2.$$

Met andere woorden, er wordt gevraagd om aan te tonen dat de recursief gedefinieerde uitdrukking in het linkerlid gelijk is aan de formule in het rechterlid, en dit voor alle waarden van n.

Om dit te bewijzen, kunnen we als volgt te werk gaan. De formule is zeker correct voor $n = 1$, aangezien $1 = 1^2$. Veronderstel dat de formule correct is voor een specifieke waarde k, met andere woorden

$$\sum_{i=1}^{k} (2i - 1) = k^2.$$

Dan is de formule ook correct voor $k + 1$, want

$$\begin{aligned} \sum_{i=1}^{k+1} (2i - 1) &= \sum_{i=1}^{k} (2i - 1) + 2k + 1 \\ &= k^2 + 2k + 1 \\ &= (k + 1)^2. \end{aligned}$$

Aangezien we reeds hebben opgemerkt dat de formule correct is voor $n = 1$, is zij bijgevolg ook correct voor $n = 2$, en om dezelfde reden is zij dan geldig voor elke andere waarde van n.

Een dergelijke bewijsvoering steunt op het *inductieprincipe*. Het is een zeer eenvoudige, maar uitermate bruikbare techniek. Het is terug een gevolg van het axioma van de goede ordening in $\mathbb{N}$ (of $\mathbb{N}^*$) dat een dergelijke bewijsvoering correct is.

Stelling 2.3.1. *Veronderstel dat S een deelverzameling van $\mathbb{N}^*$ is waarvoor*

(a) $1 \in S$;

(b) *voor elke $k \in \mathbb{N}^*$ geldt: $k \in S$ impliceert dat $k + 1 \in S$.*

Dan is $S = \mathbb{N}^*$.

Bewijs. Indien de conclusie niet waar zou zijn, en bijgevolg $S \neq \mathbb{N}^*$, dan is het complement van S t.o.v. $\mathbb{N}^*$, m.a.w. $\mathbb{N}^* \setminus S = \{r \in \mathbb{N}^* \mid r \notin S\}$ een niet-ledige deelverzameling van $\mathbb{N}^*$. Als gevolg van het axioma van de goede ordening bezit $\mathbb{N}^* \setminus S$ een kleinste element m. Aangezien echter $1 \in S$, zal $m \neq 1$. Bijgevolg is $m - 1 \in \mathbb{N}^*$, maar aangezien m het kleinste element is van $\mathbb{N}^* \setminus S$, zal $m - 1 \in S$. Stel nu $k = m - 1$ in de 2de voorwaarde van de stelling, dan volgt hieruit dat $m \in S$, bijgevolg een tegenstrijdigheid. Dus we mogen besluiten dat $S = \mathbb{N}^*$. □

Opmerkingen

1. Het feit dat het resultaat waar is voor $n = 1$ wordt soms de *inductiebasis* genoemd, terwijl de veronderstelling dat de uitdrukking waar is voor $n = k$ de *inductiehypothese* wordt genoemd. We merken ook op dat wij ook als inductiebasis $n = 0$ hadden kunnen nemen, soms zal het zelfs voorkomen dat andere waarden van n als inductiebasis zullen dienen. Van de andere kant wordt soms als inductiehypothese aangenomen dat een uitdrukking waar is voor alle waarden kleiner dan k. Men spreekt dan soms van het *sterk inductieprincipe*.

2. Het inductieprincipe kan niet in $\mathbb{Z}$ worden toegepast (waarom?).

3. Een interessante variant op het inductieprincipe is het zogenaamde *principe van het kleinste tegenvoorbeeld*. Veronderstel dat $S \subseteq \mathbb{N}^*$ een verzameling is waarvan we willen bewijzen dat $S = \mathbb{N}^*$. Dan kunnen we uit het ongerijmde tewerk gaan; als $S \neq \mathbb{N}^*$, dan bestaat er wegens het axioma van de goede ordening een *kleinste* element in $\mathbb{N}^* \setminus S$. Dit element noemen we dan het kleinste tegenvoorbeeld. Als we uit het bestaan van dit kleinste tegenvoorbeeld een contradictie krijgen, dan hebben we bewezen dat de veronderstelling $S \neq \mathbb{N}^*$ onmogelijk is, zodat we kunnen besluiten dat $S = \mathbb{N}^*$.

Oefeningen

1. Gebruik het inductieprincipe om te bewijzen dat

$$\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1).$$

2. Gebruik het inductieprincipe om te bewijzen dat

$$\sum_{i=0}^{n} 3^i = \frac{1}{2}(3^{n+1} - 1).$$

3. Maak een tabel van de waarden

$$s_n = \sum_{i=1}^{n} i^3,$$

voor $1 \leq n \leq 6$. Zoek op basis van deze tabel een formule voor s_n. Bewijs met behulp van het inductieprincipe dat deze formule correct is voor alle $n \geq 1$.

4. Gebruik het sterk inductieprincipe om aan te tonen dat u_n recursief gedefinieerd als

$$u_1 = 3, \quad u_2 = 5, \quad u_n = 3u_{n-1} - 2u_{n-2} \ (n \geq 3),$$

gelijk is aan $2^n + 1$ voor elke $n \in \mathbb{N}^*$.

5. Zoek het kleinste natuurlijk getal n_0 waarvoor geldt dat $n! \geq 2^n$. Indien $n = n_0$ als inductiebasis genomen wordt, bewijs dan het resultaat voor alle $n \geq n_0$.

6. Bewijs door middel van inductie dat

$$\sum_{i=1}^{2^n} \frac{1}{i} \geq 1 + \frac{n}{2}.$$

7. Gebruik het inductieprincipe om te bewijzen dat voor elk natuurlijk getal n, $2^{n+2} + 3^{2n+1}$ deelbaar is door 7.

2.4 Het ladenprincipe van Dirichlet

Veronderstel dat we m objecten willen verdelen over n laden, dan is het onmiddellijk duidelijk dat, indien er meer objecten zijn dan laden, er ten minste 1 lade zal zijn die meer dan 1 object bevat. Dit zeer eenvoudig principe, wordt het *ladenprincipe* genoemd, maar is ook onder verschillende andere namen gekend zoals het *duivenhokprincipe*, in het Engels wordt dit principe het *pigeonhole principle* genoemd.

Voorbeelden

Alhoewel dit een zeer eenvoudig principe is, zijn er heel wat toepassingen te bedenken van dit principe.

1. In elke verzameling van ten minste 13 mensen, zijn er ten minste 2 die verjaren in dezelfde maand.

2. In elke verzameling van 1 miljoen mensen, zijn er ten minste 2 die evenveel haren op hun hoofd hebben.

3. In elke groep mensen zijn er steeds 2 mensen te vinden die evenveel vrienden hebben. (We veronderstellen wel dat de vriendschap wederkerig is.)

   Dit laatste voorbeeld vereist, in tegenstelling tot de twee voorgaande, wel enige toelichting. Inderdaad, noem X de groep mensen, en noem f een afbeelding van X naar $\mathbb{N}$, zodanig dat $f(x)$ het aantal vrienden van $x \in X$ is. Als $|X| = m$, dan kan $f(x)$ de waarden $0, 1, \ldots, m-1$ aannemen. Met andere woorden, het waardengebied van f is een deelverzameling van $\mathbb{N}[0, m-1]$. Om het ladenprincipe te kunnen toepassen, moeten we echter nog bewijzen dat het waardengebied een eigenlijke deelverzameling is van $\mathbb{N}[0, m-1]$. Merk echter op dat, indien er een persoon a is die $m-1$ vrienden heeft (met andere woorden alle personen uit X zijn vrienden van a), dan is er geen enkel persoon uit X zonder vrienden, dus in dit geval is 0 geen element van de waardenverzameling van f, en omgekeerd als 0 tot de waardenverzameling behoort, dan zal $m-1$ er niet toe behoren. Bijgevolg is de waardenverzameling een echte deelverzameling van $\mathbb{N}[0, m-1]$ en heeft dus ten hoogste $m-1$ elementen. Nu kunnen wij het ladenprincipe toepassen en er zijn dus ten minste 2 mensen a en b uit de groep waarvoor geldt dat $f(a) = f(b)$.

Oefeningen

1. Bewijs dat een willekeurige verzameling van 12 gehele getallen ten minste 2 elementen bezit waarvan het verschil deelbaar is door 11.

2. Hoeveel elementen moet een deelverzameling van $\mathbb{N}[1, 999]$ minstens hebben om alleszins twee elementen met som 1000 te bevatten?

3. Zij gegeven een rij van m gehele getallen $a_1, a_2, a_3, \ldots, a_m$. Toon aan dat er een aantal a_i's kunnen gevonden worden zodanig dat ze in de rij mekaar opvolgen en waarvan de som deelbaar is door m.

4. Veronderstel dat X een deelverzameling is van $\mathbb{N}[1, 2n]$ die precies $n+1$ elementen bevat. Bewijs dat er steeds één van de elementen van X een deler is van een ander element van X zodanig dat het quotiënt even is.

2.5 Eindige en oneindige verzamelingen

2.5.1 Definities

Een verzameling X, zodanig dat er een bijectie bestaat van de verzameling $\mathbb{N}[1, n]$ naar X, wordt een *eindige* verzameling genoemd. We noemen n de *orde* of de *kardinalieit* van de verzameling X, en we noteren dit als $|X| = n$ of ook soms als $\#X = n$.

Elke verzameling die niet eindig is wordt een *oneindige* verzameling genoemd.

Alhoewel de volgende stelling op het eerste gezicht triviaal lijkt, is het toch de moeite hierop in te gaan.

Stelling 2.5.1. *Een niet-ledige verzameling X is een oneindige verzameling dan en slechts dan als er een injectie bestaat van $\mathbb{N}^*$ naar X.*

Bewijs. Veronderstel dat X een oneindige verzameling is. Dan kunnen wij steeds op de volgende recursieve manier een functie f van $\mathbb{N}^*$ naar X definiëren. Noem $f(1)$ een willekeurig element van X; indien $f(1), \ldots, f(k)$ gedefinieerd zijn, dan kiezen wij voor $f(k+1)$ een willekeurig element van X verschillend van $f(1), \ldots, f(k)$. Bijgevolg is f een injectie. Bovendien is $f(k+1)$ steeds gedefinieerd, want anders zou $X = \{f(1), f(2), \ldots, f(k)\}$ zodat f een bijectie zou zijn van X naar $\mathbb{N}[1, k]$, maar dit is tegen de veronderstelling dat X een oneindige verzameling is.

Veronderstel nu omgekeerd dat er een injectie f bestaat van $\mathbb{N}^*$ naar X. Indien X eindig zou zijn, dan zou er een bijectie β van $\mathbb{N}[1, n]$ naar X bestaan

voor een zekere n. Bijgevolg bestaat de volgende ketting van injecties:

$$\mathbb{N}[1, n+1] \xrightarrow{i} \mathbb{N}^* \xrightarrow{f} X \xrightarrow{\beta^{-1}} \mathbb{N}[1, n].$$

Hierbij is i de zogenaamde *inclusie-injectie* ($i(k) = k$). De samenstelling van al deze injecties, is terug een injectie α van $\mathbb{N}[1, n+1]$ naar $\mathbb{N}[1, n]$, maar dit is onmogelijk wegens het ladenprincipe. Bijgevolg moet X een oneindige verzameling zijn. □

2.5.2 Opmerking

Merk op dat de injectie f, waarvan sprake is in het bewijs van de bovenstaande stelling, niet noodzakelijk een bijectie is. Een oneindige verzameling X wordt *aftelbaar* genoemd, als er een bijectie bestaat van $\mathbb{N}^*$ naar X (we kunnen dan inderdaad de elementen *aftellen*). Indien dit niet het geval is, dan noemen we X een *niet-aftelbare* verzameling. Bijgevolg kunnen we onder de oneindige verzamelingen nog een onderscheid maken tussen de aftelbare en de niet-aftelbare verzamelingen. Het ligt voor de hand dat we eindige verzamelingen eveneens als aftelbare verzamelingen beschouwen. De theorie met betrekking tot de aftelbare verzamelingen zou men kunnen beschouwen als het domein van de discrete wiskunde, dit in tegenstelling tot de theorie met betrekking tot de niet-aftelbare verzamelingen (zoals $\mathbb{R}$, zie later) die tot het domein van de analyse behoort.

Merk op dat de oneindige verzamelingen eigenlijke deelverzamelingen kunnen bezitten die zelf oneindige verzamelingen zijn. Zo is bijvoorbeeld de verzameling van de even natuurlijke getallen een eigenlijke deelverzameling van $\mathbb{N}$.

2.5.3 Voorbeelden

1. De verzameling van de gehele getallen is aftelbaar. Inderdaad, beschouw de afbeelding f van $\mathbb{N}$ naar $\mathbb{Z}$ gedefinieerd door

$$f(n) = \begin{cases} \frac{n}{2} & \text{als } n \text{ even is} \\ -\frac{n+1}{2} & \text{als } n \text{ oneven is.} \end{cases}$$

   Deze afbeelding is inderdaad een bijectie en de geordende waardenverzameling van f, of de *rij* van de waarden is $(0, -1, 1, -2, 2, -3, 3, \ldots)$.

2. De verzameling $\mathbb{Q}$ van de rationale getallen is eveneens aftelbaar. Er bestaat inderdaad terug een bijectie f van $\mathbb{N}$ naar $\mathbb{Q}$ waarvan de rij van

waarden er als volgt uitziet:

$$(0, -1, 1, -2, -1/2, 1/2, 2, -3, -3/2, -1/3, 1/3, 2/3, 3/2, 3, \dots).$$

Om de plaats van a/b in deze rij te bepalen, gaan we als volgt te werk. We bepalen eerst zogenaamde *niveaus*. Op niveau 0 komt enkel het getal 0. Voor het bepalen van de andere niveaus veronderstellen wij dat de breuk een onvereenvoudigbare breuk is met $a \neq 0$ en dat $b > 0$. Wij noemen $n = \max(|a|, b)$ (met $|a|$ de absolute waarde van a) het niveau van de breuk a/b. Per niveau worden alle rationale getallen op dit niveau gerangschikt volgens de orderelatie $<$ van $\mathbb{Q}$. Op die manier ontstaat een lijst van de volgende gedaante.

niveau								
0	0							
1	-1	1						
2	-2	$-1/2$	$1/2$	2				
3	-3	$-3/2$	$-2/3$	$-1/3$	$1/3$	$2/3$	$3/2$	3
4	-4	$-4/3$	$-3/4$	$-1/4$	$1/4$	$3/4$	$4/3$	4
$\vdots$	$\vdots$							

Elk rationaal getal komt op die manier juist één maal voor in deze lijst. Aangezien er nu voor elk natuurlijk getal n slechts een eindig aantal rationale getallen a/b bestaan van niveau $n = \max(|a|, b)$, volgt hieruit dat $\mathbb{Q}$ inderdaad aftelbaar is.

3. De verzameling $\mathbb{R}$ is een niet-aftelbare verzameling. We bewijzen dit door aan te tonen dat het interval $[0, 1]$ van $\mathbb{R}$ een niet-aftelbare verzameling is, en we gebruiken hiervoor *Cantor's diagonaalmethode*.

   Veronderstel dus het tegendeel, met andere woorden, veronderstel dat $[0, 1]$ wel aftelbaar zou zijn. Dan is er een bijectie f van $\mathbb{N}$ naar het interval $[0, 1]$, en ontstaan de volgende waarden:

$$\begin{aligned} f(0) &= 0.a_0b_0c_0d_0\dots \\ f(1) &= 0.a_1b_1c_1d_1\dots \\ f(2) &= 0.a_2b_2c_2d_2\dots \\ f(3) &= 0.a_3b_3c_3d_3\dots \\ &\vdots \end{aligned}$$

   Hierbij staan $a_i, b_i, \dots$ voor één van de cijfers 0 tot en met 9.

We produceren nu een reëel getal tussen 0 en 1 dat niet in de lijst kan voorkomen. We noemen

$$x = 0.x_1x_2x_3x_4\ldots$$

waarbij

$$x_1 = \begin{cases} a_0 + 1 & \text{als } a_0 \leq 8 \\ 0 & \text{als } a_0 = 9 \end{cases}$$

$$x_2 = \begin{cases} b_1 + 1 & \text{als } b_1 \leq 8 \\ 0 & \text{als } b_1 = 9 \end{cases}$$

$$x_3 = \begin{cases} c_2 + 1 & \text{als } c_2 \leq 8 \\ 0 & \text{als } c_2 = 9 \end{cases}$$

$$\vdots$$

Als bijvoorbeeld de lijst vanwaar wij vertrekken op de volgende manier begint:

$$\begin{array}{l} 0.772563\ldots \\ 0.092971\ldots \\ 0.000000\ldots \\ 0.000722\ldots \\ 0.000998\ldots \\ 0.227354\ldots \\ \vdots \end{array}$$

Dan zal het getal x beginnen als $0.801805\ldots$. De juiste definitie van x doet er niet toe, het is alleen belangrijk om te bewijzen dat x niet in de lijst getallen waarvan wij vertrokken zijn, kan voorkomen. Inderdaad, voor $n = 0, 1, 2, \ldots$ zal het getal x met het getal $f(n)$ verschillen op de $(n+1)$-ste plaats na de komma. Bijgevolg zal het interval $[0, 1]$ en dus ook de verzameling $\mathbb{R}$ niet aftelbaar zijn.

Opmerking

Het feit dat $\mathbb{Q}$ aftelbaar is, kan misschien meer verwonderlijk schijnen dan voor $\mathbb{Z}$ aangezien er tussen elke 2 rationale getallen oneindig veel andere rationale getallen gelegen zijn. Het bewijs steunt echter op een volledige andere ordening dan de natuurlijke ordening $<$ van de rationale getallen.

2.5.4 Kardinaalgetallen

Opmerking 2.5.2 stelt ons in staat om een definitie te geven van *het kardinaalgetal* van een verzameling. We noemen een verzameling X en een verzameling Y *gelijkmachtig* (notatie $X \sim Y$) dan en slechts dan als er een bijectie bestaat van X naar Y. De relatie $\sim$ is duidelijk een equivalentierelatie. We noemen het *kardinaalgetal* $|X|$ van X de equivalentieklasse $(X)_\sim$ van de verzameling X onder deze equivalentierelatie $\sim$. Indien de verzameling X een eindige verzameling is, dan is $X \sim \mathbb{N}[1, n]$ voor een zekere n, en is dus $\mathbb{N}[1, n]$ een representant voor de equivalentieklasse $|X|$. We stellen daarom kort $|X| = n$. Voor de oneindige verzamelingen ligt dit enigszins anders. Inderdaad, we hebben gezien dat er tussen 2 oneindige verzamelingen niet altijd een bijectie bestaat. Beschouwen we nu de verzameling $\mathbb{N}$, we noteren het kardinaalgetal van deze verzameling (en van elke verzameling die hiermee bijectief is) als $\aleph_0$ (aleph-nul). Beschouw nu de afbeelding f gedefinieerd door $f(n) = n+1$, $\forall n \in \mathbb{N}$. Dan is f een bijectie van $\mathbb{N}$ naar $\mathbb{N}^*$, en bijgevolg is $|\mathbb{N}^*| = |\mathbb{N}| = \aleph_0$. Anderzijds is

$$\mathbb{N} = \mathbb{N}^* \cup \{0\},$$

zodat, indien we de optelling van eindige kardinaalgetallen tot de oneindige kardinaalgetallen willen uitbreiden,

$$\aleph_0 = \aleph_0 + 1.$$

Dit betekent bijvoorbeeld dat bij het rekenen met oneindige kardinaalgetallen de schrappingswet niet geldt, want anders zou $0 = 1$.

De theorie van de oneindige kardinaalgetallen werd ontwikkeld door Georg Cantor (1845–1918). De ogenschijnlijke paradox is het gevolg van het feit dat er bijecties bestaan van de verzameling $\mathbb{N}$ naar eigenlijke deelverzamelingen van $\mathbb{N}$.

2.6 Het vereenvoudigd somprincipe

Dit principe is evenals het ladenprincipe vrij triviaal. Het luidt als volgt:

> *Als A_i $(i = 1, \ldots, k)$ k twee aan twee disjuncte, eindige verzamelingen zijn, dan is*
>
> $$|A_1 \cup A_2 \cup \ldots \cup A_k| = \sum_{i=1}^{k} |A_i|.$$

(Bewijs dit principe door te steunen op het inductieprincipe.) Dit principe geeft ons de mogelijkheid om het ladenprincipe in een meer algemene vorm te formuleren:

> *Indien m objecten over n laden moeten verdeeld worden waarbij $m > nr$, dan is er ten minste één lade die meer dan r objecten bevat.*

Oefeningen

1. Bewijs dat in elke groep van 6 personen er steeds 3 mensen kunnen gevonden worden die ofwel mekaar ooit eens ontmoet hebben, ofwel mekaar nooit ontmoet hebben.

2. In het eenheidsvierkant liggen 51 punten. Bewijs dat er een cirkelschijf met straal 1/7 bestaat die minstens 3 van de punten bedekt.

2.7 Het productprincipe

Veronderstel dat X en Y twee eindige verzamelingen zijn met $|X| = n$ en $|Y| = m$. Beschouw een willekeurige relatie S tussen X en Y, m.a.w. S is een willekeurige deelverzameling van de *productverzameling*

$$X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}.$$

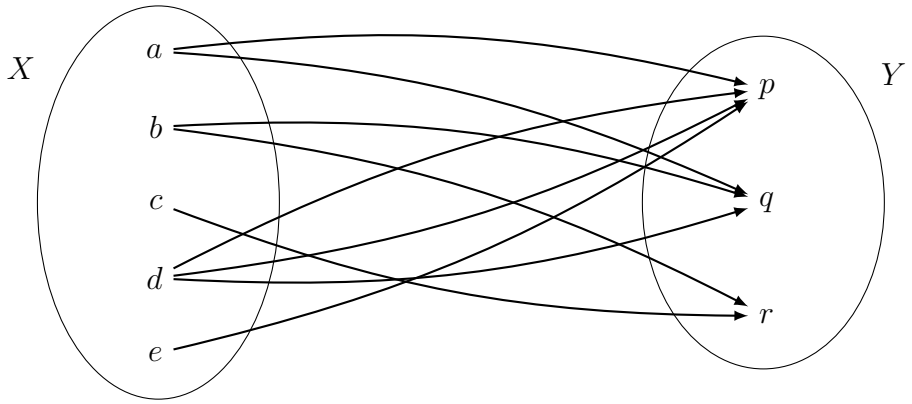
Indien we nu de kardinaliteit van deze eindige verzameling S willen bepalen, dan kunnen wij op twee manieren te werk gaan. Men kan met name eerst alle koppels tellen die een welbepaalde x als eerste element bevatten. Noem $r_x(S)$ het aantal koppels in S die x als eerste element bevatten. Dan is

$$|S| = \sum_{x \in X} r_x(S).$$

Noem anderzijds $k_y(S)$ het aantal koppels in S die y als tweede element bevatten. Dan is

$$|S| = \sum_{y \in Y} k_y(S).$$

Voorbeeld



$$2+2+1+3+1 \qquad = \qquad 4+3+2$$

Deze telmethode is op het eerste gezicht zeer eenvoudig, maar heeft heel wat toepassingen. Wij vatten deze methode in de volgende stelling samen.

Stelling 2.7.1. *Indien X en Y twee eindige niet-ledige verzamelingen zijn, en indien S een deelverzameling is van $X \times Y$, dan gelden volgende eigenschappen.*

(1) *(Het principe van de dubbele telling.) De orde van S wordt gegeven door*

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} k_y(S).$$

(2) *Indien $r_x(S)$ een constante r is, onafhankelijk van de keuze van $x \in X$, en indien $k_y(S)$ een constante k is, onafhankelijk van de keuze van $y \in Y$, dan is*

$$r|X| = k|Y|.$$

(3) *(Het productprincipe.) De orde van $X \times Y$ wordt gegeven door*

$$|X \times Y| = |X| \cdot |Y|.$$

(Bewijs als oefening)

Voorbeeld

Op een feestje zijn 15 *jongens en een onbekend aantal meisjes. Elke jongen kent juist* 4 *meisjes, en elk meisje kent juist* 6 *jongens op het feestje. Hoeveel meisjes zijn er?*

Oplossing.
Stel X gelijk aan de verzameling van de jongens op het feestje en Y de verzameling van de meisjes; zij S de relatie "kennen elkaar". We passen Stelling 2.7.1(2) toe. In ons geval is $r = 4$ en $k = 6$, en dus verkrijgen we uit $r|X| = k|Y|$ dat $4 \cdot 15 = 6 \cdot |Y|$. We besluiten dat $|Y| = 10$; er zijn dus 10 meisjes op het feest.

Oefeningen

1. Veronderstel dat we een aantal verschillende deelverzamelingen van $\mathbb{N}[1, 8]$ beschouwen zodanig dat elke deelverzameling 4 elementen bevat en dat elk element van $\mathbb{N}[1, 8]$ tot 3 dergelijke deelverzamelingen behoort. Hoeveel dergelijke deelverzamelingen zijn er dan?

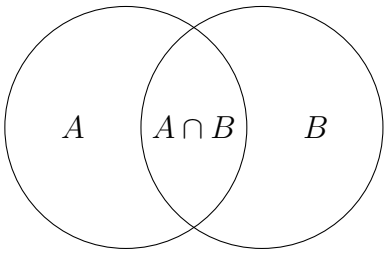
2. Is het mogelijk om een verzameling van deelverzamelingen van $\mathbb{N}[1, 8]$ te vinden zodanig dat elke deelverzameling 3 elementen bevat, en zodanig dat elk element van $\mathbb{N}[1, 8]$ tot 5 deelverzamelingen behoort?

3. Indien $X_1, X_2, \ldots, X_n$ verzamelingen zijn (eventueel gelijk), dan wordt
$$X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i\}$$
de productverzameling van $X_1, X_2, \ldots, X_n$ genoemd. Bewijs door middel van het inductieprincipe dat
$$|X_1 \times X_2 \times \cdots \times X_n| = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_n|.$$

2.8 Het eenvoudig inclusie-exclusie principe

Dit principe is een uitbreiding van het vereenvoudigd somprincipe. In zijn eenvoudigste versie kan men dit principe als volgt formuleren:

Stelling 2.8.1. *Als A en B twee eindige verzamelingen zijn, dan geldt*
$$|A \cup B| = |A| + |B| - |A \cap B|.$$



We komen later terug op een algemene versie van dit principe.

Voorbeeld

Hoeveel natuurlijke getallen van 1 *tot en met* 1000 *zijn niet deelbaar door* 3 *noch door* 7*?*

Oplossing.
Noteer V_3 en V_7 voor de verzamelingen van de drievouden, resp. de zevenvouden, kleiner dan of gelijk aan 1000. Het antwoord op de vraag wordt gegeven door

$$1000 - |V_3 \cup V_7| \,.$$

Blijft nu het bepalen van $|V_3 \cup V_7|$. Het is duidelijk dat $|V_3| = 333$ en dat $|V_7| = 142$. Verder geldt eveneens $V_3 \cap V_7 = V_{21}$ (de verzameling van de 21-vouden) en $|V_{21}| = 47$. Het antwoord op de vraag vinden we dus als

$$1000 - (333 + 142 - 47) = 572.$$

2.9 Combinatieleer

Traditioneel wordt onder *combinatieleer* het tellen van al dan niet geordende k-tallen verstaan. Hierbij kunnen in deze k-tallen al dan niet herhalingen optreden. We geven hier een kort overzicht van deze theorie.

2.9.1 Variaties

Voorbeeld

Een voetbaltoernooi wordt door 4 ploegen gespeeld (we noemen ze a, b, c, d). Telkens wordt een thuis- en een uitwedstrijd gespeeld. Veronderstel dat we een wedstrijd waarbij ploeg a als thuisploeg speelt tegen de ploeg b (als uitploeg) noteren als ab. Hoeveel wedstrijden moeten er gespeeld worden?

Er wordt dus gevraagd naar het aantal koppels bestaande uit verschillende elementen, die we kunnen maken uit de verzameling $X = \{a, b, c, d\}$. In dit geval zijn deze koppels eenvoudig uit te schrijven. Het zijn er 12, met name

$$\begin{array}{cccc} ab & ba & ca & da \\ ac & bc & cb & db \\ ad & bd & cd & dc \end{array}$$

Definitie

Een *variatie van n elementen in groepen van k* is een **geordend** k-tal van k **verschillende** elementen gekozen uit een gegeven **verzameling** van n

elementen. Het totaal aantal variaties van n elementen in groepen van k noteren we door V_n^k of nog door $P(n,k)$.

Opmerkingen

1. Het is duidelijk dat $k \leq n$; $k \in \mathbb{N}$ en $n \in \mathbb{N}$. Hierbij veronderstellen we stilzwijgend dat indien $k = 0$, $V_n^0 = 1$.
2. Twee verschillende variaties van n elementen in groepen van k kunnen dus verschillend zijn
   - door de opgenomen elementen;
   - door de volgorde van de elementen.

Stelling 2.9.1. *Voor alle $n, k \in \mathbb{N}$ met $k \leq n$ geldt*

$$V_n^k = n(n-1)\cdots(n-(k-1))\,.$$

Bewijs. Aangezien de volgorde van belang is, en aangezien een element geen 2 maal in een variatie kan voorkomen, kunnen we als volgt te werk gaan. We kiezen eerst het eerste element, dat kan op n verschillende manieren, eens het eerste element gekozen, blijven er nog $n-1$ manieren over om het tweede element te kiezen, waarna er nog $n-2$ manieren zijn om het derde element te kiezen. Indien wij zo verder gaan, zullen er voor de laatste keuze (met name de $k$de keuze) nog $n-(k-1)$ kandidaten overblijven. In het totaal zijn er dus $n(n-1)\cdots(n-(k-1))$ mogelijke variaties van n elementen in groepen van k. □

Permutaties

Een bijzonder en vaak voorkomend geval van variaties is de situatie waarbij $k = n$.

Definitie

Een variatie van n elementen in groepen van n, wordt een *permutatie* genoemd. Met andere woorden, het is een geordend n-tal van n verschillende elementen. Twee permutaties van n elementen zijn dus verschillend door de **volgorde** van de elementen. Het is duidelijk dat het aantal permutaties van n elementen gelijk is aan

$$P(n,n) = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1.$$

Zoals we reeds vroeger gezien hebben, wordt dit aantal kort voorgesteld door $n!$ (n-faculteit).

Opmerkingen

1. We spreken af dat $0! = 1$.

2. Uit de formule van het aantal variaties van n elementen in groepen van k volgt duidelijk dat dit kan geschreven worden als

$$V_n^k = \frac{n!}{(n-k)!}.$$

   Merk terloops op dat, indien we $k = 0$ stellen in de bovenstaande formule, $V_n^0 = \frac{n!}{n!} = 1$, hetgeen de eerdere afspraak rechtvaardigt. Anderzijds is $0! = 1$ in overeenstemming met

$$V_n^n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!.$$

3. Het woord permutatie is uiteraard goed gekozen. Inderdaad, een permutatie van n elementen is niets anders dan een bijectie van een verzameling met n elementen op zichzelf. De verzameling van alle permutaties van een verzameling met n elementen stellen we voor door S_n of $\mathsf{Sym}(n)$.

2.9.2 Combinaties

Voorbeeld

Veronderstel dat bij het voetbaltoernooi tussen de 4 ploegen a, b, c, d telkens slechts 1 wedstrijd (op neutraal terrein) wordt gespeeld. In dit geval speelt de volgorde dus geen rol. We zoeken in dit geval nu naar het aantal **paren** uit de verzameling van 4 elementen. Dit aantal is uiteraard 6.

Definitie

Een *combinatie van n elementen in groepen van k* is een **deelverzameling** met k elementen uit een gegeven verzameling van n elementen. Het aantal combinaties van n elementen in groepen van k stellen we voor door $\binom{n}{k}$, C_n^k of $C(n,k)$. Deze getallen worden ook nog de *binomiaalgetallen* of de *binomiaalcoëfficiënten* genoemd.

Stelling 2.9.2. *Voor alle $n, k \in \mathbb{N}$ met $k \leq n$ geldt*

$$V_n^k = \binom{n}{k} \cdot k!\,.$$

Bewijs. Een willekeurige variatie van n elementen in groepen van k ontstaat door eerst een deelverzameling met k elementen uit de verzameling van deze n elementen te nemen, en dit kan op $\binom{n}{k}$ manieren, en daarna de volgorde van de k elementen in deze deelverzameling vast te leggen. We kunnen deze k elementen op $k!$ manieren permuteren, m.a.w. we kunnen deze k elementen op $k!$ manieren ordenen. In het totaal kunnen we dus op die manier $\binom{n}{k}k!$ variaties construeren. □

Gevolg

$$\binom{n}{k} = \frac{V_n^k}{k!} = \frac{n!}{(n-k)!\,k!}\,.$$

Eigenschappen

1. Voor alle $n, k \in \mathbb{N}$ met $k \leq n$ geldt

   $$\binom{n}{k} = \binom{n}{n-k}\,.$$

   Dit volgt onmiddellijk uit de bovenstaande formule, maar kan ook onmiddellijk uit de definitie afgeleid worden.

2. Voor alle $n, k \in \mathbb{N}$ met $k \leq n$ geldt

   $$\binom{n}{k+1} = \binom{n}{k} \cdot \frac{n-k}{k+1}\,.$$

   Inderdaad,

   $$\begin{aligned}\binom{n}{k+1} &= \frac{n!}{(k+1)!(n-(k+1))!} \\ &= \frac{n!}{k!(n-k)!} \cdot \frac{n-k}{k+1} \\ &= \binom{n}{k} \cdot \frac{n-k}{k+1}.\end{aligned}$$

3. Voor alle $n, k \in \mathbb{N}^*$ met $k < n$ geldt de formule van Stifel–Pascal:

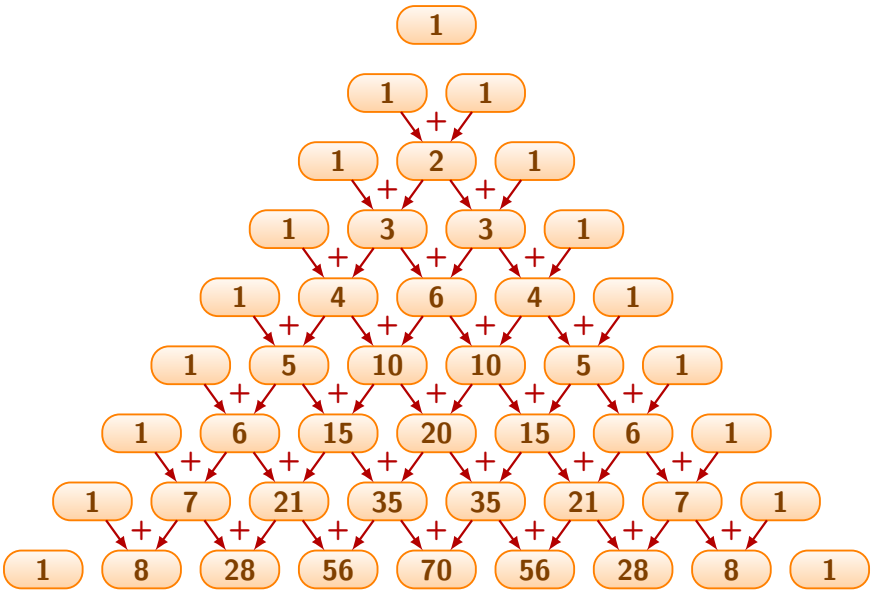
   $$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}\,. \tag{2.1}$$

   Inderdaad, indien we uit de verzameling van n elementen één element a fixeren, dan kunnen al de mogelijke combinaties van de n elementen

in groepen van k ingedeeld worden in twee disjuncte verzamelingen. Enerzijds zijn er de combinaties die a bevatten. Een dergelijke combinatie vormen we door uit de $n-1$ overblijvende elementen $k-1$ andere elementen te kiezen. Het aantal is $\binom{n-1}{k-1}$. Anderzijds zijn er de combinaties die a niet bevatten, zo een combinatie vormen we door uit de $n-1$ overblijvende elementen er juist k uit te kiezen, hun aantal is $\binom{n-1}{k}$. Hieruit volgt de formule.

De driehoek van Pascal

Uit de formule $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ $(n, k \in \mathbb{N}^*,\ k < n)$, volgt een recursieve methode om de binomiaalgetallen $\binom{n}{k}$ te berekenen, indien de binomiaalgetallen $\binom{n-1}{k}$, $0 \leq k \leq n-1$, gekend zijn. De getallen worden veelal in een driehoek gerangschikt. Deze driehoek wordt soms de driehoek van Pascal genoemd, naar Blaise Pascal (1623–1662).



2.9.3 Herhalingsvariaties

Zoals het woord het zelf zegt, zal in dit geval een element in een geordend k-tal meerdere malen mogen voorkomen. De definitie luidt dus als volgt.

Definitie

Een *herhalingsvariatie van n elementen in groepen van k* is een **geordend** k-tal elementen uit een verzameling van n elementen. Het aantal herhalingsvariaties van n elementen in groepen van k noteren we door $\overline{V_n^k}$ of $\overline{P(n,k)}$.

Stelling 2.9.3. *Voor alle $n, k \in \mathbb{N}$ met $n \geq 1$ geldt*

$$\overline{V_n^k} = n^k.$$

Bewijs. Dit is onmiddellijk duidelijk, aangezien bij elke nieuwe keuze, al de elementen uit de verzameling van n elementen gekozen mogen worden. □

Opmerking

Het is duidelijk dat hier in tegenstelling tot het geval van de variaties zonder herhaling, k kleiner dan, gelijk aan of groter dan n kan zijn.

2.9.4 Herhalingscombinaties

Definitie

Een *herhalingscombinatie van n elementen in groepen van k* is een **niet-geordend** k-tal elementen, gekozen uit een verzameling van n elementen. Het aantal dergelijke herhalingscombinaties wordt voorgesteld door $\overline{\binom{n}{k}}$ of nog door $\overline{C(n,k)}$.

Een herhalingscombinatie ontstaat dus door uit een voorraad van n voorwerpen $a_1, a_2, \ldots, a_n$ precies k voorwerpen uit te kiezen. Herhaling is mogelijk maar de volgorde is niet van belang. In het algemeen zal zo'n keuze er dus als volgt uitzien: men heeft bijvoorbeeld r_1 keer het voorwerp a_1 gekozen, r_2 keer het voorwerp a_2, …, r_n keer het voorwerp a_n. Vermits in totaal k voorwerpen gekozen werden, geldt uiteraard dat $r_1 + r_2 + r_3 + \cdots + r_n = k$. We kunnen dus stellen

> Het aantal herhalingscombinaties van n elementen in groepen van k is gelijk aan het aantal manieren waarop we een natuurlijk getal k kunnen schrijven als de som van n natuurlijke getallen $r_1, r_2, \ldots, r_n$.

Stelling 2.9.4. *Voor alle $n, k \in \mathbb{N}$ met $n \geq 1$ geldt*

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

Bewijs. Aangezien de volgorde geen belang heeft kunnen we dus in elk k-tal al de elementen van dezelfde soort samen plaatsen. We maken ons hiervan nu de volgende voorstelling. We beschikken over n hokjes waarover we k stippen verdelen. Indien we de hokjes afscheiden door middel van een schot (rechte streep), dan hebben we hiervoor $n-1$ schotten nodig. Het probleem is dus herleid tot het opvullen van $n-1+k$ plaatsen met k stippen en $n-1$ rechte strepen. Indien we eerst de k stippen plaatsen, dan moeten de overige $n-1$ plaatsen ingenomen worden door strepen. Bijgevolg is het voldoende om na te gaan op hoeveel manieren we $n-1+k$ plaatsen kunnen opvullen met k stippen (of gelijkwaardig hiermee: op hoeveel manieren we $n-1+k$ plaatsen kunnen opvullen met $n-1$ strepen). Met andere woorden, het probleem is herleid tot de vraag op hoeveel manieren we uit een verzameling van $n-1+k$ plaatsen er k kunnen selecteren. Dit is uiteraard het aantal combinaties van $n-1+k$ elementen in groepen van k (of gelijkwaardig: in groepen van $n-1$). □

Samenvatting

De verschillende tellingen die we hier besproken hebben, hangen af van de manier van kiezen van de elementen; met name

- met of zonder terugplaatsen van de gekozen elementen,
- met of zonder rekening te houden met de volgorde.

We kunnen de resultaten als volgt samenvatten:

	zonder terugplaatsen	met terugplaatsen
ongeordend	$\binom{n}{k}$	$\binom{n+k-1}{k}$
geordend	$n(n-1)\cdots(n-k+1)$	n^k

2.10 Toepassingen op combinatieleer

2.10.1 Het aantal deelverzamelingen van een verzameling

Stelling 2.10.1. *Een verzameling X van n elementen bezit 2^n deelverzamelingen.*

Bewijs. Noem $X = \{x_1, x_2, \ldots, x_n\}$ en beschouw de verzameling $Y = \{0, 1\}$. Met elke deelverzameling S van X kunnen we nu een functie f_S van X naar Y laten corresponderen, die als volgt gedefinieerd wordt.

$$f_S(x_i) = \begin{cases} 0 & \text{als } x_i \notin S\,, \\ 1 & \text{als } x_i \in S\,. \end{cases}$$

Het aantal deelverzamelingen van X is bijgevolg gelijk aan het aantal manieren waarop we uit een verzameling Y met 2 elementen geordende n-tallen kunnen kiezen. Dit is bijgevolg gelijk aan het aantal herhalingsvariaties van 2 elementen in groepen van n, dus aan 2^n. □

2.10.2 Het binomium van Newton

De volgende formules maken deel uit van de zogenaamde reeks merkwaardige producten

$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Deze formules zijn bijzondere gevallen van het zogenaamde *binomium van Newton.*

Stelling 2.10.2. *Veronderstel dat n een positief natuurlijk getal is, dan geldt voor elke twee (reële) getallen a en b, dat*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Bewijs. Het bewijs van deze stelling is zeer eenvoudig. De formule volgt eigenlijk uit de manier waarop we, met behulp van de distributieve eigenschap, het product met n factoren $(a+b)(a+b)\cdots(a+b)$ uitrekenen. De coëfficiënt van $a^k b^{n-k}$ is het aantal manieren om uit de n factoren $(a+b)$, k maal a te kiezen (en dus $n-k$ maal b). Dit is het aantal combinaties van n elementen in groepen van k, dus $\binom{n}{k}$. □

Opmerking

1. Het doet er niet toe of a en b reële getallen zijn, we hebben enkel gesteund op de commutativiteit van de vermenigvuldiging.

2. Volgende vormen zijn allemaal equivalente vormen van het binomium van Newton (bewijs dit als oefening).

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{n-k} a^k b^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\ &= \sum_{k=0}^{n} \binom{n}{n-k} a^{n-k} b^k \,.\end{aligned}$$

Oefeningen

1. Bewijs het binomium van Newton door gebruik te maken van inductie.

2. Bewijs de volgende formules:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$
$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

3. Bewijs de volgende formule:

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

4. Bewijs dat het binomiaalgetal $\binom{p}{k}$ met p een priemgetal, deelbaar is door p voor elke waarde van k, $1 \leq k \leq p-1$. Leid hieruit af dat $(a+b)^p - a^p - b^p$ steeds deelbaar is door p voor elke 2 gehele getallen a en b.

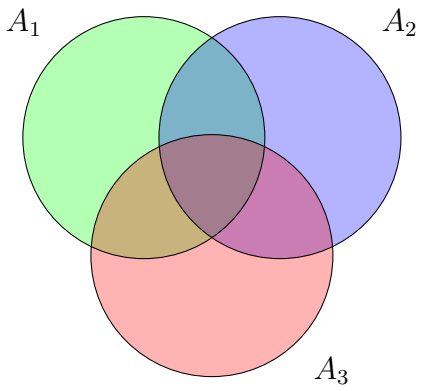
2.10.3 Het (veralgemeend) inclusie-exclusie principe

We hebben in het vereenvoudigd inclusie-exclusie principe gezien dat voor de kardinaliteit van de unie van 2 verzamelingen A_1 en A_2 geldt:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Beschouwen we 3 verzamelingen A_1, A_2 en A_3, dan moeten we naast de orde van de doorsneden $A_1 \cap A_2$, $A_1 \cap A_3$, $A_2 \cap A_3$, ook rekening houden met de orde van de doorsnede $A_1 \cap A_2 \cap A_3$ en dan geldt:

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



Deze formules kunnen we nu samenvatten in het zogenaamde (veralgemeend) *inclusie-exclusie principe* of *zeefprincipe*.

Stelling 2.10.3. *Als $A_1, A_2, \ldots, A_n$ eindige verzamelingen zijn, dan is*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{n-1}\alpha_n.$$

Hierbij is α_i de notatie voor de som van de kardinaalgetallen van al de mogelijke doorsneden die men kan vormen met i dergelijke verzamelingen A_i. We kunnen dit ook nog herschrijven als

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{S \subseteq \{1,\ldots,n\}} (-1)^{|S|-1} \left| \bigcap_{j \in S} A_j \right|.$$

Bewijs. We bewijzen dat elk element x uit de unie inderdaad slechts 1 maal wordt geteld in het rechterlid. Veronderstel dat x tot juist k verzamelingen behoort. Dan zal x een bijdrage k leveren in $\alpha_1 = \sum_{i=1}^{n} |A_i|$. In de som

$\alpha_2 = \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$ zal de bijdrage 1 zijn dan en slechts dan als A_i en A_j zich onder de k verzamelingen bevinden die x bevatten. Er zijn $\binom{k}{2}$ dergelijke paren verzamelingen $\{A_i, A_j\}$, bijgevolg is $\binom{k}{2}$ de bijdrage van x tot α_2. Algemeen is $\binom{k}{i}$ de bijdrage van x in α_i. De totale bijdrage van x in het rechterlid is bijgevolg

$$\binom{k}{1} - \binom{k}{2} + \cdots + (-1)^{k-1}\binom{k}{k}.$$

Aangezien echter (zie oefeningen)

$$\sum_{i=0}^{k}(-1)^i\binom{k}{i} = 0$$

volgt hieruit dat de bijdrage van x tot het rechterlid juist 1 is. □

Oefening

Geef een alternatief bewijs van Stelling 2.10.3 met behulp van het inductieprincipe.

2.10.4 Permutaties zonder fixelementen: wanorde

Een weinig efficiënte secretaresse moet n brieven in n omslagen doen. Op hoeveel manieren kan ze erin slagen om alle brieven in verkeerde omslagen te doen?

We vragen dus in feite het aantal permutaties van de verzameling $\mathbb{N}[1, n]$ die geen enkel fixelement bezitten. Een dergelijke permutatie wordt een *wanorde* genoemd. Volgens het inclusie-exclusie principe is het totaal aantal wanordes d_n van $\mathbb{N}[1, n]$ gelijk aan[1]

$$d_n = n! - \alpha_1 + \alpha_2 - \cdots + (-1)^n\alpha_n,$$

waarbij α_i de som is van het aantal permutaties van $\mathbb{N}[1, n]$ die i gegeven elementen fixeren, voor alle mogelijke keuzes van i elementen uit $\mathbb{N}[1, n]$. Er zijn nu $\binom{n}{i}$ manieren om i elementen te kiezen uit $\mathbb{N}[1, n]$, en het aantal permutaties van $\mathbb{N}[1, n]$ die deze i elementen (elementsgewijze) fixeren is het aantal permutaties op de $n-i$ overige elementen, met andere woorden $(n-i)!$. Bijgevolg is

$$\alpha_i = \binom{n}{i} \cdot (n-i)! = \frac{n!}{i!},$$

[1] In de notatie van Stelling 2.10.3 is dus elke A_k gelijk aan de verzameling van alle permutaties die het element "k" fixeren.

zodat het totaal aantal wanordes gelijk is aan

$$d_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right).$$

We willen nu echter een recursieve definitie van het getal d_n vinden; we geven hiervoor twee verschillende methoden.

Eerste methode

Een eerste methode bestaat erin om rechtstreeks de bekomen formule voor d_n verder te analyseren. We vinden dat

$$\begin{aligned} d_n &= n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-1} \frac{1}{(n-1)!}\right) + (-1)^n \frac{n!}{n!} \\ &= n \cdot (n-1)! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-1} \frac{1}{(n-1)!}\right) + (-1)^n \\ &= n d_{n-1} + (-1)^n . \end{aligned}$$

Dit is reeds een bevredigende recursieve formule, maar we kunnen die nog op een interessante manier herwerken:

$$\begin{aligned} d_n &= n d_{n-1} + (-1)^n \\ &= (n-1) d_{n-1} + d_{n-1} + (-1)^n \\ &= (n-1) d_{n-1} + (n-1) d_{n-2} + (-1)^{n-1} + (-1)^n \end{aligned}$$

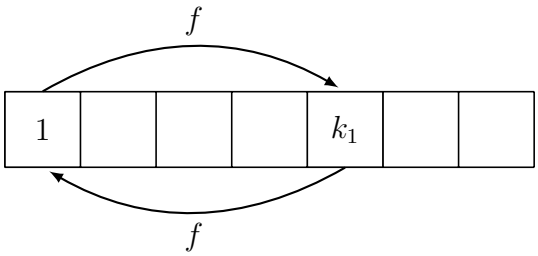
en dus

$$d_n = (n-1)(d_{n-1} + d_{n-2}) . \tag{2.2}$$

Tweede methode

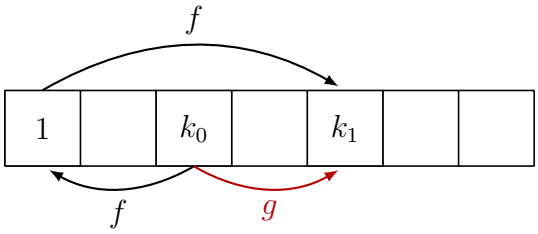
Een tweede methode om deze formule te bekomen, is conceptueler, en geeft een inzichtelijke verklaring voor de eenvoudige formule (2.2). Beschouw daartoe een willekeurige wanorde f van $\mathbb{N}[1, n]$. Aangezien geen enkel element van $\mathbb{N}[1, n]$ gefixeerd wordt, is het beeld van het element 1 het getal $f(1) = k_1$ met $k_1 \neq 1$. We vestigen onze gedachten nu op het element k_1. Er kunnen twee gevallen optreden: ofwel is $f(k_1) = 1$ (m.a.w. $f^2(1) = 1$)) ofwel is $f(k_1) \neq 1$. We tellen nu beide soorten wanordes.

Indien $f(k_1) = 1$, dan zal f een wanorde definiëren op de verzameling $\mathbb{N}[2, n] \setminus \{k_1\}$.



Het aantal dergelijke wanordes is per definitie gelijk aan d_{n-2}. Merk op dat elke wanorde op $\mathbb{N}[2,n] \setminus \{k_1\}$ aanleiding geeft tot juist 1 wanorde op $\mathbb{N}[1,n]$ door de definitie $f(1) = k_1$; $f(k_1) = 1$.

Veronderstel nu dat f een wanorde is waarvoor geldt dat $f(k_1) \neq 1$; dan bestaat er een (unieke) $k_0 \in \mathbb{N}[2,n] \setminus \{k_1\}$ zodanig dat $f(k_0) = 1$.



We definiëren nu een nieuwe permutatie g in $\mathbb{N}[2,n]$ door $g(k_0) = k_1$ en $g(k) = f(k)$ voor alle $k \neq k_0$; we slaan dus als het ware het element "1" over. Dan is g eveneens een wanorde, maar nu op de verzameling $\mathbb{N}[2,n]$, en zo zijn er d_{n-1}. Omgekeerd, als g een wanorde van $\mathbb{N}[2,n]$ is, dan is er een unieke k_0 met $g(k_0) = k_1$, en we definiëren dan een nieuwe permutatie f als volgt:

$$f(k) = \begin{cases} 1 & \text{als } k = k_0\,; \\ k_1 & \text{als } k = 1\,; \\ g(k) & \text{als } k \in \mathbb{N}[2,n] \setminus \{k_0\}\,. \end{cases}$$

Dan is f een wanorde van $\mathbb{N}[1,n]$ met $f(1) = k_1$, en beide constructies zijn elkaars invers. Er zijn dus precies d_{n-1} dergelijke wanordes.

Bijgevolg is het aantal wanordes f waarvoor geldt dat $f(1) = k_1 \in \mathbb{N}[2,n]$ (met k_1 een vast gekozen getal) gelijk aan $d_{n-1} + d_{n-2}$. Aangezien er nu $n-1$ mogelijke keuzes zijn voor k_1, zal

$$d_n = (n-1)(d_{n-1} + d_{n-2})\,;$$

we vinden dus de formule (2.2) terug.

Merk op dat $d_1 = 0$ terwijl $d_2 = 1$, zodat we op die manier een recursieve definitie gegeven hebben van het aantal wanordes op een verzameling van n elementen. We vinden de volgende waarden van d_n voor $n \leq 8$:

n	1	2	3	4	5	6	7	8
d_n	0	1	2	9	44	265	1854	14833

2.11 De Stirling getallen

Het *Stirling getal* $S(n,k)$ (van de tweede soort[2]) is per definitie het aantal mogelijkheden waarop men een verzameling X met n elementen kan schrijven als een disjuncte unie van k niet-ledige deelverzamelingen.

Stelling 2.11.1. *Het Stirling getal $S(n,k)$ met $1 \leq k \leq n$ wordt recursief gedefinieerd door*

$$\begin{aligned} &S(n,1) = 1 \\ &S(n,k) = S(n-1,k-1) + kS(n-1,k) \quad (2 \leq k \leq n-1) \\ &S(n,n) = 1\,. \end{aligned}$$

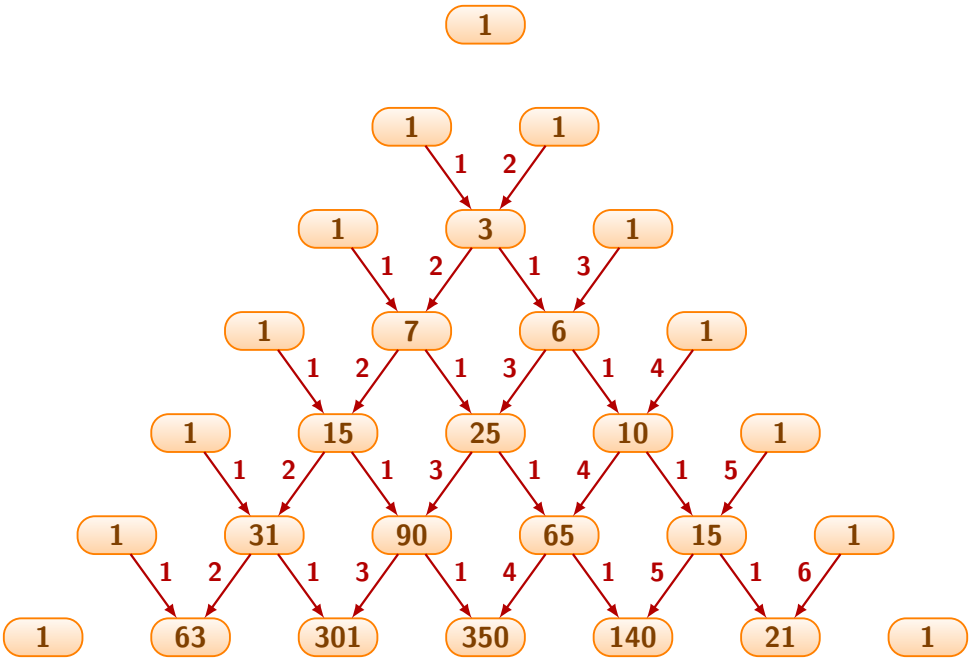
Bewijs. Het is duidelijk dat $S(n,1) = S(n,n) = 1$. Veronderstel nu dat $2 \leq k \leq n-1$. Noem z een willekeurig element van X. Indien we al de mogelijke partities van X in k klassen beschouwen, dan zal ofwel (i) het singleton $\{z\}$ een klasse van de partitie zijn ofwel (ii) zal $\{z\}$ een eigenlijke deelverzameling zijn van één klasse. Indien we in het eerste geval $\{z\}$ wegnemen uit de partitie, dan ontstaat een partitie van de verzameling $X \setminus \{z\}$ in $k-1$ klassen. Het aantal dergelijke partities is $S(n-1,k-1)$. Omgekeerd zal elke partitie $\mathcal{P}$ van $X \setminus \{z\}$ in $k-1$ klassen, op unieke manier een partitie van X in k klassen definiëren door aan $\mathcal{P}$ het singleton $\{z\}$ toe te voegen. Indien we echter in het tweede geval z wegnemen uit de partitie, dan ontstaat een partitie van de verzameling $X \setminus \{z\}$ in k klassen. Omgekeerd, beschouw een partitie $\mathcal{P}$ van de verzameling $X \setminus \{z\}$ in k klassen. Dan kunnen we hieruit k verschillende partities in k klassen van de verzameling X construeren door het element z achtereenvolgens toe te voegen aan elke klasse van $\mathcal{P}$. Hieruit mogen we besluiten dat er $k \cdot S(n-1,k)$ partities van de tweede soort zijn.

Het totaal aantal partities van een verzameling van n elementen in k klassen is bijgevolg gelijk aan

$$S(n,k) = S(n-1,k-1) + kS(n-1,k) \quad (2 \leq k \leq n-1). \qquad \square$$

[2]Er bestaan ook Stirling getallen van de eerste soort, maar die laten we hier buiten beschouwing.

Naar analogie met de driehoek van Pascal voor binomiaalgetallen kan er ook een driehoek voor de Stirling getallen van de tweede soort opgesteld worden.



Gevolg

Het aantal surjecties van een verzameling X met n elementen naar een verzameling Y met k elementen is gelijk aan $k!\,S(n,k)$. (Bewijs als oefening).

Oefeningen

Bewijs de volgende identiteiten voor de Stirling getallen.

$$S(n,2) = 2^{n-1} - 1$$

$$S(n,n-1) = \binom{n}{2}$$

$$S(n,k) = \sum_{i=0}^{n-1} \binom{n-1}{i} S(i,k-1)\,.$$

2.12 De multinomiaalgetallen

Veronderstel dat we een verzameling X met n verschillende objecten hebben, en dat we die willen kleuren in k verschillende kleuren, maar zodanig dat het aantal objecten dat we in een gegeven kleur $i \in \mathbb{N}[1,k]$ willen kleuren, gelijk is aan een vast aantal n_i. (Uiteraard kan dit enkel als $\sum_{i=1}^{k} n_i = n$.) Het aantal mogelijke dergelijke kleuringen noemen we een *multinomiaalgetal*, en we noteren dit aantal[3] als

$$\binom{n}{n_1, n_2, \ldots, n_k}.$$

Merk op dat

$$\binom{n}{n_1, n_2} = \binom{n}{n_1},$$

vandaar de benaming multinomiaalgetallen als veralgemening van de binomiaalgetallen.

Stelling 2.12.1. *Als $n, n_1, \ldots, n_k$ positieve natuurlijke getallen zijn waarvoor $\sum_{i=1}^{k} n_i = n$, dan is*

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1!\, n_2! \cdots n_k!}.$$

Bewijs. Zij $X = \mathbb{N}[1,n]$, en beschouw een *vaste kleuring* c van X in k verschillende kleuren met n_i elementen in elke kleur i, bijvoorbeeld de elementen $1, \ldots, n_1$ in kleur 1, vervolgens $n_1 + 1, \ldots, n_1 + n_2$ in kleur 2, enzovoort.

Beschouw eerst een willekeurige permutatie van X. Door deze permutatie te laten inwerken op de vaste kleuring c bekomen we een nieuwe geldige kleuring van X, die we zullen noteren als $f(c)$. Het is duidelijk dat elke mogelijke geldige kleuring kan bekomen worden door de vaste kleuring "door elkaar te haspelen"; elke geldige kleuring is dus van de vorm $f(c)$ voor een zekere permutatie f van X.

We moeten nog na gaan hoe vaak we elke geldige kleuring op die manier kunnen bekomen. Als f en g twee permutaties zijn zodat $f(c)$ en $g(c)$ identieke kleuringen zijn, dan verschillen deze twee permutaties enkel van elkaar door het permuteren van elementen van eenzelfde kleur. Voor elke kleur i

[3] Een nog iets formelere definitie van het multinomiaal getal is dat dit het aantal functies is van een verzameling X met n elementen op een verzameling $Y = \{y_1, y_2, \ldots, y_k\}$, zodanig dat y_i het beeld is van n_i elementen uit X. De elementen $y_1, \ldots, y_k$ spelen dus de rol van de k verschillende kleuren.

zijn er precies n_i elementen in deze kleur, en deze kunnen op $n_i!$ manieren onderling gepermuteerd worden. We kunnen dus elke mogelijke kleuring precies $n_1!n_2!\cdots n_k!$ keer verkrijgen.

Uit het principe van de dubbele telling (zie Stelling 2.7.1(2)) volgt nu dat het aantal geldige kleuringen gelijk is aan

$$\frac{n!}{n_1!\,n_2!\cdots n_k!}.$$ □

Aangezien de multinomiaalgetallen de veralgemening zijn van de binomiaalgetallen, is het niet verwonderlijk dat er een veralgemening bestaat van het binomium van Newton, met name de *multinomiaalstelling*.

Stelling 2.12.2. *Voor elke 2 positieve natuurlijke getallen n en k geldt dat*

$$\Big(\sum_{i=1}^{k} a_i\Big)^n = \sum \binom{n}{n_1, n_2, \ldots, n_k} a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}.$$

Hierbij wordt de som in het rechterlid genomen over al de mogelijke k-tallen van natuurlijke getallen $(n_1, n_2, \ldots, n_k)$ waarvoor $\sum_{i=1}^{k} n_i = n$.

Bewijs. De coëfficiënt van $a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ in de ontwikkeling is het aantal keer dat we uit de n factoren $(a_1 + a_2 + \cdots + a_k)$, de term a_1 nemen uit n_1 van de factoren, de term a_2 nemen uit n_2 van de factoren, ..., de term a_k nemen uit n_k van de factoren. Dit is juist de definitie van de multinomiaalgetallen. Hieruit volgt het gestelde. □

Oefeningen

1. Hoeveel woorden (eventueel zonder betekenis) van 11 letters kunnen we maken met de letters uit het woord MISSISSIPPI?

2. Indien $a + b + c = n$, bewijs dan dat

$$\binom{n}{a, b, c} = \binom{n-1}{a-1, b, c} + \binom{n-1}{a, b-1, c} + \binom{n-1}{a, b, c-1}.$$

3. Veronderstel dat p een priemgetal is. Bewijs dat het multinomiaalgetal

$$\binom{p}{n_1, n_2, \ldots, n_k}$$

deelbaar is door p tenzij één van de getallen n_i gelijk is aan p.

4. Bewijs dat
$$S(n,k) = \frac{1}{k!} \sum \binom{n}{n_1, n_2, \ldots, n_k}$$
waarbij de som genomen wordt over alle k-tallen $(n_1, n_2, \ldots, n_k)$ van positieve natuurlijke getallen waarvan de som n is.

5. Op hoeveel manieren kan men mn voorwerpen verdelen over m dozen zodanig dat elke doos juist n elementen bevat?

6. Bewijs, door gebruik te maken van de multinomiaalgetallen, dat

   (a) 2^n een deler is van $(2n)!$ en dat het quotiënt even is;

   (b) $(n!)^{n+1}$ een deler is van $(n^2)!$.

   (c) $(n!)^{2n+1}$ een deler is van $(n^2!)!$.

Hoofdstuk

3 Discrete probabiliteit

Sommigen van jullie hebben wellicht al gehoord van hashtabellen (hash tables) of hashfuncties (hash maps). We geven het idee aan door middel van een voorbeeld.

In een boekenwinkel kan men boeken bestellen, en men dient daarvoor een formulier in te vullen, waarop men naast de nodige informatie over het boek, ook persoonlijke gegevens invult, zoals naam, adres, telefoonnummer, enz. De boekenhandelaar houdt het formulier bij, bestelt het boek, en wanneer het boek is toegekomen informeert hij de klant dat hij zijn boek kan komen ophalen. Deze bestelling kan natuurlijk een paar dagen of weken in beslag nemen, en intussen loopt het aantal verzamelde formulieren flink op, laten we zeggen tot een duizendtal formulieren. Als de klant dan terugkomt en de handelaar moet het desbetreffende formulier terugvinden, zou het natuurlijk zeer onpraktisch zijn om door al die formulieren te moeten gaan zoeken naar het juiste exemplaar. Ook het alfabetisch sorteren (bv. op familienaam) is niet echt praktisch, enerzijds omdat het telkens wat tijd in beslag neemt om een nieuw formulier op de juiste plaats te steken, en anderzijds omdat men toch nog steeds in één grote stapel moet gaan zoeken.

De boekenhandelaar heeft een slimme methode bedacht om dit proces efficiënter te maken. Hij heeft achter zijn toonbank een rooster gemaakt van 10 bij 10, dus met 100 vakjes in, die hij genummerd heeft van 00 tot en met 99, waarin hij formulieren kan leggen. Als hij een nieuw formulier ontvangt, kijkt hij naar het telefoonnummer van de klant, neemt de 2 laatste cijfers ervan, en legt het formulier in het overeenkomstige vakje. Als de klant dan enkele dagen later zijn boek komt ophalen, geeft hij zijn telefoonnummer, en in het overeenkomstige vakje liggen hooguit een dozijn formulieren, waar de boekenhandelaar onmiddellijk het juiste formulier kan uithalen. Aangezien we verwachten dat de laatste twee cijfers van een telefoonnummer zich "uniform willekeurig" gedragen, kan verwacht worden dat op elk moment alle vakjes min of meer een vergelijkbaar aantal formulieren zal bevatten.

Dit eenvoudig voorbeeld geeft het principe weer van een *hashfunctie*, dat in de computerwereld niet meer weg te denken is. In plaats van een rooster achter een toonbank gebruikt men een tabel (de *hashtabel*) met m genummerde locaties, die *buckets* of *slots* genoemd worden, en elk daarvan bevat

een lijst met data items. Elk item heeft een unieke identifier, die de *key* genoemd wordt. Wanneer een nieuw data item in de hashtabel moet opgeslagen worden, wordt de *hashfunctie* h berekend van de key, die als resultaat weergeeft in welke bucket dit item thuishoort (de *hash* van dit item).

Een goede hashfunctie moet de items zo gelijkmatig mogelijk verdelen over de buckets. In ons voorbeeld zijn de items de formulieren, de keys de telefoonnummers, en de hashfunctie is de afbeelding die een telefoonnummer afbeeldt op de laatste twee cijfers ervan. We verwachten dat dit een goede hashfunctie is, in tegenstelling tot bijvoorbeeld de afbeelding die een telefoonnummer zou afbeelden op de eerste twee cijfers ervan, omdat deze streekgebonden zijn en we dus geen gelijkmatige verdeling verwachten in onze (lokale) boekenwinkel.

Het is dus belangrijk om te kunnen inschatten in hoeverre een gegeven afbeelding gelijkmatig verdeelde resultaten teruggeeft. In ons voorbeeld van telefoonnummers is dit intuïtief wel duidelijk, maar voor complexere data zal het noodzakelijk zijn dit op een gegronde manier te kunnen analyseren.

We zullen ook andere voorbeelden tegenkomen die duidelijk maken dat probabiliteitstheorie belangrijk is in de praktijk. Wanneer het noodzakelijk is om bijvoorbeeld geneste lussen te schrijven om een hoeveelheid gegevens te verwerken, kan het zeer nuttig zijn om te kunnen inschatten wat de verwachte uitvoertijd is, en een andere volgorde of andere opbouw van het programma kan resulteren in een veel grotere performantie.

3.1 Toevalsgebeurtenissen

Definities

Om kansen te kunnen toekennen aan gebeurtenissen, moeten we een duidelijk beeld hebben van wat deze gebeurtenissen zijn. We zullen dus een model voorstellen van het soort situaties waarin het aannemelijk is om te spreken van probabiliteiten of kansen, en we zullen onze vragen en probleemstellingen over kansen dan vertalen naar probleemstellingen over dit model.

We spreken van de *uitkomstenruimte* om te verwijzen naar de verzameling van alle mogelijke uitkomsten van een bepaald proces. In de discrete probabiliteitstheorie veronderstellen we steeds dat deze uitkomstenruimte *eindig* is, bv. de 52 kaarten in een kaartspel, de mogelijke hashes in een hashtabel, het resultaat bij het gooien van één of meerdere dobbelstenen, de mogelijke antwoorden op een meerkeuzevragenexamen, enzomeer.

Zoals bij elke verzameling zullen we de items van de uitkomstenruimte

elementen noemen. Als we bijvoorbeeld een vragenlijst krijgen met drie vragen waarop we "ja" (J) of "neen" (N) moeten antwoorden, dan wordt de uitkomstenruimte van deze vragenlijst gegeven door

$$S = \{\text{JJJ}, \text{JJN}, \text{JNJ}, \text{JNN}, \text{NJJ}, \text{NJN}, \text{NNJ}, \text{NNN}\}\,.$$

Een deelverzameling van de uitkomstenruimte (bestaande uit één of meerdere elementen) noemen we een *gebeurtenis*, en ook de elementen zelf noemen we vaak gebeurtenissen. Zo wordt in het vorige voorbeeld de gebeurtenis "het antwoord op de eerste twee vragen is ja" gegeven door de deelverzameling $\{\text{JJJ}, \text{JJN}\}$.

Twee gebeurtenissen A en B worden *disjunct* genoemd als $A \cap B = \emptyset$, m.a.w. als de gebeurtenissen niet tegelijk kunnen optreden. Zo zijn in bovenstaand voorbeeld de gebeurtenissen "het antwoord op de eerste twee vragen is ja" en "het antwoord op de laatste twee vragen is neen" disjunct, maar de gebeurtenissen "het antwoord op de eerste vraag is ja" en "het antwoord op de laatste vraag is neen" zijn niet disjunct.

Om kansen te berekenen, kennen we een *probabiliteitsgewicht* $P(x)$ toe aan elk element x van de uitkomstenruimte. Er zijn twee regels die we daarbij moeten aanhouden:

- Elk gewicht is een reëel getal gelegen in het interval $[0, 1]$;
- de som van de gewichten van alle elementen van de uitkomstenruimte is 1.

We definiëren dan de kans $P(E)$ van een gebeurtenis E als de som van de gewichten van de elementen van E:

$$P(E) = \sum_{x \in E} P(x)\,.$$

We noemen P een *probabiliteitsfunctie* op de uitkomstenruimte S. Merk op dat deze functie P voldoet aan de volgende eigenschappen.

- $P(A) \geq 0$ voor elke $A \subseteq S$;
- $P(S) = 1$;
- $P(A \cup B) = P(A) + P(B)$ voor elke twee *disjuncte* gebeurtenissen A en B.

Elke functie P op een verzameling die aan deze drie eigenschappen voldoet, noemen we een *probabiliteitsdistributie* of *probabiliteitsmaat*. Merk op dat het toekennen van een probabiliteitsmaat op een verzameling S equivalent is met het toekennen van probabiliteitsgewichten aan elk van de elementen (met inachtname van de twee gegeven regels).

Voorbeelden

1. Wanneer we een muntstuk opgooien, is het aannemelijk om de kans op "kop" en "munt" gelijk te stellen. We definiëren dus een kansfunctie P op de uitkomstenruimte $\{\mathrm{K}, \mathrm{M}\}$ door $P(\mathrm{K}) = P(\mathrm{M}) = 1/2$ te stellen. Dit is natuurlijk niet de enige mogelijke kansfunctie op deze verzameling, maar wel de enige waarbij de probabiliteit van beide elementen gelijk is.

2. Veronderstel dat we een muntstuk drie keer opgooien. De uitkomstenruimte bevat dan $2^3 = 8$ elementen, die (bij een eerlijk muntstuk) elk met kans $1/8$ zullen optreden. De kans op de gebeurtenis "er wordt juist 1 keer kop gegooid" is dan $3/8$, want precies 3 van de 8 elementen van de uitkomstenruimte voldoen hieraan.

3. Veronderstel dat we een lijst van k keys willen hashen in een tabel met n buckets. De uitkomstenruimte bestaat dan uit alle mogelijke rijen van k elementen die elk een waarde uit $\{1, \ldots, n\}$ aannemen; dit is dus een verzameling bestaande uit n^k elementen. Als de hashfunctie goed gekozen is, is de probabiliteit van elk van deze uitkomsten gelijk aan $1/n^k$. We zeggen dat er een *botsing* (collision of clash) is tussen twee keys als ze dezelfde hash waarde hebben.

   Wat is de kans dat de k keys een verschillende hash waarde hebben? Het aantal uitkomsten die tot deze gebeurtenis behoren, kunnen we eenvoudig bepalen: deze elementen zijn precies de variaties van n elementen in groepen van k, en het aantal is dus gelijk aan $V_n^k = n!/(n-k)!$. De kans dat de k keys een verschillende hash waarde hebben is dus

$$\frac{n!}{(n-k)! \cdot n^k}\,.$$

   Het is interessant om deze waarde eens te berekenen voor verschillende waarden van n en k. Zo is de kans dat er bij het hashen van 10 keys in 20 buckets geen botsing optreedt, gelijk aan

$$\frac{20!}{10! \cdot 20^{10}} \approx 0.0655\,,$$

   en is de kans dat er bij het hashen van 50 keys in 100 buckets geen botsing optreedt, gelijk aan

$$\frac{100!}{50! \cdot 100^{50}} \approx 0.000000307\,.$$

   Deze resultaten zijn misschien niet onmiddellijk wat je intuïtief zou verwachten!

Complementaire gebeurtenissen

Zij S een uitkomstenverzameling. Dan worden twee gebeurtenissen E en F *complementair* genoemd, als $E \cap F = \emptyset$ en $E \cup F = S$, m.a.w. als E en F complementair zijn als deelverzamelingen van S. Het complement van een gebeurtenis E (binnen de uitkomstenverzameling S) wordt vaak genoteerd als E^{c}. Het volgend resultaat is zeer eenvoudig maar eveneens zeer nuttig.

Stelling 3.1.1. *Als E en F twee complementaire gebeurtenissen zijn, dan is*

$$P(F) = 1 - P(E)\,.$$

Bewijs. Dit volgt onmiddellijk uit de eigenschappen van P; meer bepaald hebben we $1 = P(S) = P(E \cup F) = P(E) + P(F)$ omdat E en F disjuncte gebeurtenissen zijn. □

Beschouw bijvoorbeeld het experiment waarbij we 10 keer een muntstuk opgooien. Wat is de kans dat we minstens 2 keer kop gooien? In principe kunnen we dit oplossen door

$$P(E) = P(2 \times \mathrm{K}) + P(3 \times \mathrm{K}) + \cdots + P(10 \times \mathrm{K})$$

te berekenen, maar het is veel eenvoudiger om de complementaire gebeurtenis te beschouwen, met name $F =$ "ten hoogste 1 keer kop gooien". Uit de vorige stelling volgt dan dat

$$\begin{aligned} P(E) = 1 - P(F) &= 1 - P(0 \times \mathrm{K}) - P(1 \times \mathrm{K}) \\ &= 1 - 1/1024 - 10/1024 = 1013/1024\,. \end{aligned}$$

Uniforme probabiliteitsmaten

We noemen P een *uniforme probabiliteitsmaat* of een *uniforme probabiliteitsdistributie* als elk element van de uitkomstenruimte hetzelfde probabiliteitsgewicht heeft. We hebben onmiddellijk het volgend resultaat, dat we in feite al hebben toegepast in de voorgaande voorbeelden.

Stelling 3.1.2. *Veronderstel dat P een uniforme probabiliteitsmaat is op een uitkomstenruimte S. Dan geldt voor elke gebeurtenis $E \subseteq S$ dat*

$$P(E) = \frac{|E|}{|S|}\,.$$

Bewijs. Stel $S = \{x_1, \ldots, x_n\}$, met $n = |S|$; dan is, voor elke $i \in \{1, \ldots, n\}$,

$$1 = P(S) = P(x_1) + \cdots + P(x_n) = n \cdot P(x_i)\,,$$

en dus is $P(x_i) = 1/n$. Voor elke $E \subseteq S$ geldt dan

$$P(E) = \sum_{x \in E} P(x) = \sum_{x \in E} \frac{1}{n} = \frac{|E|}{n}\,. \qquad \square$$

Opmerking 3.1.3. De voorwaarde dat de probabiliteitsmaat uniform moet zijn, is uiteraard van cruciaal belang. Stel bijvoorbeeld dat we gooien met twee dobbelstenen, en als uitkomstenruimte $S = \{2, 3, \ldots, 12\}$ beschouwen. Deze verzameling bevat 11 elementen. Echter, de kans om minder dan 5 te gooien (dus $P(E)$ met $E = \{2, 3, 4\}$) is niet gelijk aan 3/11, maar wel aan 1/6 (ga dit zelf na door een betere uitkomstenverzameling te kiezen).

Oefeningen

1. Als we willekeurig vijf kaarten trekken uit een volledig kaartspel (zonder teruglegging), wat is dan de kans dat we vijf kaarten van dezelfde kleur trekken? (Met "kleur" bedoelen we de vier kaartkleuren harten, ruiten, klaveren en schoppen.)

2. We gooien gelijktijdig met drie onvervalste dobbelstenen. Wat is de kans dat de som van de ogen even is? En wat is de kans dat het product van de ogen even is?

3. Welk van de volgende drie gebeurtenissen is het meest waarschijnlijk, en welke het minst waarschijnlijk?

   (a) Een aas en een koning trekken, wanneer we twee kaarten trekken uit de 13 schoppenkaarten;

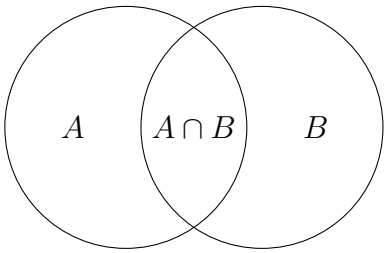
   (b) Een aas en een koning trekken, wanneer we twee kaarten trekken uit alle 52 kaarten;

   (c) Een aas en een koning van dezelfde kleur trekken, wanneer we twee kaarten trekken uit alle 52 kaarten;

3.2 Unies en doorsneden

Als A en B twee disjuncte gebeurtenissen zijn, dan is de kans dat minstens één van beide zich voordoet, gelijk aan de som van de kans dat A zich voordoet

met de kans dat B zich voordoet: $P(A \cup B) = P(A) + P(B)$. Maar wat als A en B niet disjunct zijn?



Het is duidelijk dat $A \cup B$ de disjuncte unie is van de delen $A \setminus B$, $A \cap B$ en $B \setminus A$, en uit de gekende eigenschap voor de probabiliteit van een disjuncte unie halen we

$$\begin{aligned} P(A \cup B) &= P(A \setminus B) + P(A \cap B) + P(B \setminus A) \\ &= \big(P(A \setminus B) + P(A \cap B)\big) + \big(P(B \setminus A) + P(A \cap B)\big) - P(A \cap B) \\ &= P(A) + P(B) - P(A \cap B)\,. \end{aligned}$$

We herkennen hierin het inclusie-exclusie principe voor de kardinaliteiten van twee eindige verzamelingen A en B, dat we gezien hebben in sectie 2.8. Net zoals we dat principe veralgemeend hebben naar het algemene inclusie-exclusie principe (zie Stelling 2.10.3), zo kunnen we ook onze voorgaande probabiliteitsformule veralgemenen.

Stelling 3.2.1 (Inclusie-exclusie principe voor probabiliteiten)**.** *Zij S een uitkomstenruimte met een probabiliteitsmaat P. Dan geldt, voor elk stel gebeurtenissen $E_1, \ldots, E_n$, dat*

$$P\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{i_1, i_2, \ldots, i_k \\ 1 \le i_1 < i_2 < \cdots < i_k \le n}} P\left(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}\right)\,.$$

Bewijs. Volledig analoog aan het bewijs van Stelling 2.10.3. □

Opmerking 3.2.2. In heel wat gevallen kan het eenvoudiger zijn om in plaats van het inclusie-exclusie principe toe te passen, over te gaan naar de complementaire gebeurtenissen. Inderdaad, als $E_1, \ldots, E_n$ gebeurtenissen zijn, dan is

$$\bigcup_{i=1}^{n} E_i = \left(\bigcap_{i=1}^{n} E_i^{\mathrm{c}}\right)^{\mathrm{c}}\,,$$

en dit is vaak gemakkelijker te berekenen dan het inclusie-exclusie principe toe te passen, uiteraard gebruik makend van de gekende formule $P(E^{\mathrm{c}}) = 1 - P(E)$.

Voorbeeld

We gooien tegelijk met drie dobbelstenen. Wat is de kans dat we ten minste één zes gooien?

Oplossing.
Stel, voor elke $i \in \{1,2,3\}$, E_i gelijk aan de gebeurtenis dat we een zes gooien met de i-de dobbelsteen, en E de gebeurtenis dat we ten minste één zes gooien; de gezochte kans is dan $P(E) = P(E_1 \cup E_2 \cup E_3)$. Uit het inclusie-exclusie principe halen we

$$\begin{aligned} P(E_1 \cup E_2 \cup E_3) = P(E_1) + P(E_2) + P(E_3) - P(E_1 \cap E_2) \\ - P(E_1 \cap E_3) - P(E_2 \cap E_3) + P(E_1 \cap E_2 \cap E_3)\,. \end{aligned}$$

We zien onmiddellijk in dat $P(E_i) = 1/6$ voor elke i, dat $P(E_i \cap E_j) = 1/36$ voor elke $i \neq j$, en dat $P(E_1 \cap E_2 \cap E_3) = 1/216$; we bekomen dus dat de gezochte kans gelijk is aan

$$P(E) = 3 \cdot 1/6 - 3 \cdot 1/36 + 1/216 = 91/216\,.$$

Op alternatieve wijze kunnen we deze oplossing bekomen door over te gaan naar de complementaire gebeurtenis, namelijk de gebeurtenis dat we geen enkele zes gooien. Van de $6^3 = 216$ mogelijke uitkomsten zijn er $5^3 = 125$ die geen zes bevatten, en dus is

$$P(E) = 1 - P(E^{\mathrm{c}}) = 1 - 125/216 = 91/216\,,$$

en we bekomen inderdaad hetzelfde resultaat als hierboven.

Het "hatcheck" probleem

Het volgende probleem is beroemd. In een chic restaurant komen n oude heren binnen, die allemaal een hoed op hebben. Ze leggen elk hun hoed in het hoedenrek. Bij het verlaten van het restaurant nemen ze willekeurig een hoed uit het hoedenrek, zetten die op hun hoofd, en verlaten het restaurant. Wat is de kans dat ten minste één heer de juiste hoed opheeft? Als n groter en groter wordt, zal deze kans dan naar 1 naderen?

Als uitkomstenruimte S nemen we de verzameling van alle mogelijke manieren waarop de n heren de n hoeden kunnen opzetten, en dus is $|S| = n!$. De aandachte lezer zal opgemerkt hebben dat het complement van de gebeurtenis $E =$ "minstens één heer heeft de juiste hoed op" de gebeurtenis $F =$ "geen enkele heer heeft de juiste hoed op" is, en dat dit precies overeenkomt met de mogelijke *wanordes* van de n hoeden (zie paragraaf 2.10.4 op p. 40).

Het aantal wanordes van n elementen is gelijk aan

$$d_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right),$$

en dus is de kans op de gebeurtenis "geen enkele heer heeft de juiste hoed op" gelijk aan

$$P(F) = \frac{d_n}{n!} = 1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}. \tag{3.1}$$

De kans dat minstens één heer de juiste hoed op heeft is dus

$$P(E) = 1 - P(F) = \frac{1}{1!} - \frac{1}{2!} + \cdots + (-1)^{n+1} \frac{1}{n!}. \tag{3.2}$$

Als je in de analyse al eerder reeksontwikkelingen hebt gezien, zal je deze reeksen ongetwijfeld herkennen. Inderdaad, de reeksontwikkeling van de functie $x \mapsto e^x$ wordt gegeven door

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

Het rechterlid van de formule (3.1) is dus precies de benadering van e^{-1} tot aan graad n, en als n naar oneindig gaat, zal de kans $P(E)$ dichter en dichter naderen tot $1 - e^{-1} \approx 0.632$. We zien dus dat de kans niet naar 1 nadert, in tegenstelling tot wat onze intuïtie ons misschien zou vertellen!

Oefeningen

1. Als we een onvervalst muntstuk vijf keer opgooien, wat is dan de kans dat we kop gooien op de eerste of op de laatste worp (of beide)?

2. Een groep van n getrouwde hetero-koppels zit aan een ronde tafel met $2n$ stoelen, waarbij elke persoon op een willekeurige plaats gaat zitten. Wat is de kans dat geen enkel koppel naast elkaar zit?

3. Als we in voorgaand probleem veronderstellen dat mannen en vrouwen elkaar afwisselen bij het plaatsnemen, wat is dan de kans dat geen enkel koppel naast elkaar zit? (Dit probleem staat bekend als het *mènage probleem.*)

3.3 Voorwaardelijke kans

Om het concept voorwaardelijke kans uit te leggen, beginnen we met een voorbeeld.

We gooien geblinddoekt met twee dobbelstenen. Een vriend (die niet geblinddoekt is) vertelt ons dat de som van de ogen gelijk is aan 10. Wat is de kans dat we met één van de dobbelstenen een zes gegooid hebben? Stel A gelijk aan de gebeurtenis om ten minste één zes te gooien, en B gelijk aan de gebeurtenis dat de som der ogen gelijk is aan 10. We vragen ons dus af wat de kans is dat A zich voordoet, *onder de bijkomende voorwaarde* dat B zich voordoet; we noteren deze kans als $P(A \mid B)$.

De oplossing van het probleem bestaat erin om de uitkomstenruimte S, die gelijk is aan alle mogelijke resultaten bij het gooien van twee dobbelstenen, nu te beperken tot B (want de bijkomende voorwaarde vertelt ons precies dat de gebeurtenis B zich voordoet). Om de kans $P(A \mid B)$ te bepalen, moeten we dus bepalen voor hoeveel van de uitkomsten in B de gebeurtenis A zich voordoet. In ons voorbeeld is $B = \{(4,6), (5,5), (6,4)\}$, en de uitkomsten van B waarbij gebeurtenis A zich voordoet, zijn $(4,6)$ en $(6,4)$. We zien dus dat $P(A \mid B) = 2/3$.

Het is nu duidelijk hoe we dit algemeen moeten bepalen. Inderdaad, de uitkomsten van B waarbij ook A zich voordoet, zijn precies de uitkomsten die in $A \cap B$ zitten. We stellen dus

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \, .$$

We passen deze formule ter controle nog eens rechtstreeks toe op ons voorbeeld. We hebben $P(B) = 3/36$ en $P(A \cap B) = 2/36$, en we vinden inderdaad opnieuw $P(A \mid B) = \frac{2/36}{3/36} = 2/3$.

Opmerking

Als $P(B) = 0$, dan is $P(A \mid B)$ volgens de bovenstaande formule onbepaald. We stellen in dat geval $P(A \mid B) = P(A)$; dit komt overeen met onze intuitie dat de kans dat A zich voordoet, ongewijzigd blijft onder de bijkomende voorwaarde van een gebeurtenis die zich toch niet kan voordoen.

Voorbeeld

Aan twee softwarebedrijven Micro en Soft wordt de opdracht gegeven om een eerste ontwerp te maken voor een nieuw softwarepakket. Uit vroegere ervaring is bekend dat

- *de kans dat Micro in het opzet slaagt, gelijk is aan* $2/3$*;*
- *de kans dat Soft in het opzet slaagt, gelijk is aan* $1/2$*;*
- *de kans dat ten minste één van beide bedrijven in het opzet slaagt, gelijk is aan* $3/4$*.*

Uiteindelijk blijkt juist één van beide bedrijven te slagen in het opzet. Wat is de kans dat het Micro is?

Oplossing.
Stel F gelijk aan de gebeurtenis dat beide bedrijven falen, M gelijk aan de gebeurtenis dat Micro slaagt en Soft faalt, S gelijk aan de gebeurtenis dat Soft slaagt en Micro faalt, en B gelijk aan de gebeurtenis dat beide bedrijven slagen. Uit de gegevens halen we dat

$$P(M)+P(B) = 2/3\,, \quad P(S)+P(B) = 1/2\,, \quad P(M)+P(S)+P(B) = 3/4\,.$$

Uiteraard weten we bovendien dat

$$P(F) + P(M) + P(S) + P(B) = 1\,,$$

en we leiden uit dit alles af dat

$$P(F) = 1/4\,, \quad P(M) = 1/4\,, \quad P(S) = 1/12\,, \quad P(B) = 5/12\,.$$

Gevraagd is de kans $P(M \mid M \cup S)$, en de definitie van voorwaardelijke kans geeft ons onmiddellijk dat

$$P(M \mid M \cup S) = \frac{P(M \cap (M \cup S))}{P(M \cup S)} = \frac{P(M)}{P(M) + P(S)} = \frac{1/4}{1/4 + 1/12} = \frac{3}{4}\,.$$

De vermenigvuldigingsregel

De definitie van voorwaardelijke kans kan herschreven worden als

$$P(A \cap B) = P(A)P(B \mid A)\,,$$

en wordt dan de *vermenigvuldigingsregel* voor twee gebeurtenissen genoemd. Deze kan bovendien onmiddellijk veralgemeend worden tot een gelijkaardige regel voor meerdere gebeurtenissen.

Stelling 3.3.1 (Vermenigvuldigingsregel)**.** *Zij* $A_1, \ldots, A_n$ *gebeurtenissen; dan geldt*

$$P\left(\bigcap_{i=1}^{n} A_i\right) = P(A_1)\, P(A_2 \mid A_1)\, P(A_3 \mid A_1 \cap A_2) \cdots P(A_n \mid \cap_{i=1}^{n-1} A_i)\,.$$

Bewijs. Dit volgt onmiddellijk uit de gelijkheid

$$P\left(\bigcap_{i=1}^{n} A_i\right) = P(A_1) \cdot \frac{P(A_1 \cap A_2)}{P(A_1)} \cdot \frac{P(A_1 \cap A_2 \cap A_3)}{P(A_1 \cap A_2)} \cdots \frac{P(\cap_{i=1}^{n} A_i)}{P(\cap_{i=1}^{n-1} A_i)}\,. \qquad \square$$

De vermenigvuldigingsregel is voornamelijk nuttig bij experimenten die in verschillende fasen verlopen, waarbij gebeurtenis A_i in fase i verloopt, en afhankelijk kan zijn van wat in de voorgaande fasen is gebeurd.

Voorbeeld

We trekken één voor één vijf kaarten uit een volledig kaartspel van 52 *kaarten (zonder teruglegging). Wat is de kans dat we vijf opeenvolgende kaarten in stijgende volgorde getrokken hebben? (Neem voor het gemak aan dat de kaarten van* 1 *tot en met* 13 *genummerd zijn.)*

Oplossing.
Hoewel we dit probleem ook zouden kunnen oplossen door middel van de teltechnieken die we in het vorig hoofdstuk gezien hebben, is het eenvoudiger om de vermenigvuldigingsregel te gebruiken. Stel A_1 gelijk aan de gebeurtenis dat de eerste kaart een waarde heeft in $\{1, \ldots, 9\}$, en voor elke $i \in \{2, 3, 4, 5\}$ stellen we A_i gelijk aan de gebeurtenis dat de i-de kaart een waarde heeft die juist één hoger is dan de voorgaande kaart. De gezochte kans is dan gelijk aan $P(A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5)$. We gebruiken de vermenigvuldigingsregel, en we gaan eenvoudig na dat

$$\begin{aligned} P(A_1) &= 9/13\,, \\ P(A_2 \mid A_1) &= 4/51\,, \\ P(A_3 \mid A_1 \cap A_2) &= 4/50\,, \\ P(A_4 \mid A_1 \cap A_2 \cap A_3) &= 4/49\,, \\ P(A_5 \mid A_1 \cap A_2 \cap A_3 \cap A_4) &= 4/48\,; \end{aligned}$$

we besluiten dat

$$P(A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5) = \frac{9}{13} \cdot \frac{4}{51} \cdot \frac{4}{50} \cdot \frac{4}{49} \cdot \frac{4}{48} = \frac{8}{270725}\,.$$

Het Monty Hall probleem

De naam Monty Hall verwijst naar een oud Amerikaans TV-spelprogramma. Een kandidaat krijgt te horen dat achter één van drie gesloten deuren met gelijke kans zich een prijs bevindt. De kandidaat stelt zich op bij een deur

naar keuze, waarna de spelleider (die weet welke deur de prijs verbergt) een deur opent waarachter zich geen prijs bevindt (en verschillend is van de door de kandidaat gekozen deur). De kandidaat mag nu beslissen te blijven staan ofwel zich voor de andere nog gesloten deur op te stellen. Hij wint de prijs als die zich achter de finaal gekozen deur bevindt. Wat is voor de kandidaat de beste strategie: blijven staan, of van deur veranderen?

Als de kandidaat blijft staan, bepaalt zijn initiële keuze de winstkans, en die is gelijk aan 1/3 omdat de prijs zich met gelijke kans achter 1 van de 3 deuren bevindt.

We bepalen nu de kans op winst als de kandidaat na het openen van de deur door de spelleider, zijn keuze verandert. Indien hij oorspronkelijk voor de juiste deur stond, zal hij door te veranderen van keuze met zekerheid verliezen. De kans dat dit zich voordoet, is 1/3. Indien hij oorspronkelijk voor een verkeerde deur stond, zal hij door te veranderen van keuze met zekerheid voor de juiste deur staan (want de andere verkeerde deur werd door de spelleider geopend). De kans dat dit zich voordoet, is 2/3. Deze strategie levert hem dus een winstkans van 2/3!

De totalekansformule

Veronderstel dat de gebeurtenissen $A_1, \ldots, A_n$ een partitie vormen voor de uitkomstenruimte S (dit wil zeggen dat $A_i \cap A_j = \emptyset$ voor elke $i \neq j$, en dat $S = A_1 \cup \cdots \cup A_n$). Dan geldt voor elke gebeurtenis $B \subseteq S$ dat de gebeurtenissen $B \cap A_1, \ldots, B \cap A_n$ een partitie vormen voor B. Dit leidt onmiddellijk tot het volgend resultaat.

Stelling 3.3.2 (Totalekansformule)**.** *Veronderstel dat $A_1, \ldots, A_n$ gebeurtenissen zijn die een partitie vormen voor de uitkomstenruimte S. Dan geldt voor een willekeurige gebeurtenis $B \subseteq S$ dat*

$$P(B) = P(A_1)\,P(B \mid A_1) + \cdots + P(A_n)\,P(B \mid A_n)\,.$$

Bewijs. Uit het feit dat de gebeurtenissen $B \cap A_1, \ldots, B \cap A_n$ een partitie vormen voor B volgt onmiddellijk dat $P(B) = P(B \cap A_1) + \cdots + P(B \cap A_n)$. Het resultaat volgt nu door de vermenigvuldigingsregel toe te passen op elke term. □

Voorbeeld

In een computer zitten drie geheugenmodules van 1GB, waarvan twee van merk 1 en één van merk 2. Als we willekeurig een bit schrijven naar een

geheugenmodule van type 1, is de kans op een geheugenfout $6 \cdot 10^{-18}$*; bij geheugen van type 2 is dit* $3 \cdot 10^{-18}$*. Als we nu willekeurig een bit wegschrijven op onze computer, wat is dan de kans op een geheugenfout?*

Oplossing.
We stellen A_1 gelijk aan de gebeurtenis dat we naar een geheugenmodule van type 1 wegschrijven, en A_2 de gebeurtenis dat we naar de module van type 2 wegschrijven. Als we B gelijkstellen aan de gebeurtenis dat er zich een geheugenfout voordoet, dan is

$$\begin{aligned} P(B) = P(A_1)\,P(B \mid A_1) + P(A_2)\,P(B \mid A_2) \\ = \frac{2}{3} \cdot 6 \cdot 10^{-18} + \frac{1}{3} \cdot 3 \cdot 10^{-18} = 5 \cdot 10^{-18}\,. \end{aligned}$$

De regel van Bayes

De totalekansformule wordt vaak gebruikt in samenhang met de volgende belangrijke eigenschap die een verband legt tussen voorwaardelijke kansen van de vorm $P(A \mid B)$ en voorwaardelijke kansen van de vorm $P(B \mid A)$ waarin de gebeurtenis en de conditionerende gebeurtenis verwisseld zijn.

Stelling 3.3.3 (Regel van Bayes)**.** *Veronderstel dat* $A_1, \ldots, A_n$ *gebeurtenissen zijn die een partitie vormen voor de uitkomstenruimte* S*. Dan geldt voor een willekeurige gebeurtenis* $B \subseteq S$ *dat*

$$P(A_i \mid B) = \frac{P(A_i)\,P(B \mid A_i)}{P(B)} = \frac{P(A_i)\,P(B \mid A_i)}{P(A_1)\,P(B \mid A_1) + \cdots + P(A_n)\,P(B \mid A_n)}\,.$$

Bewijs. Merk op dat $P(A_i)\,P(B \mid A_i)$ en $P(B)\,P(A_i \mid B)$ gelijk zijn aangezien beide uitdrukkingen gelijk zijn aan $P(A_i \cap B)$; hieruit volgt de eerste gelijkheid. De tweede gelijkheid volgt uit de eerste na toepassing van de totalekansformule op $P(B)$. □

De regel van Bayes wordt vaak aangewend voor *inferentie* (inference). Men kent een aantal mogelijke gebeurtenissen die tot een bepaald effect aanleiding kunnen geven. Als men dan dat effect observeert, wil men probabilistische conclusies kunnen trekken over de oorzaak van dat effect; men zegt dat men de oorzaak *infereert*. Hiervoor wordt de regel van Bayes toegepast, waarbij de gebeurtenissen $A_1, \ldots, A_n$ met de mogelijke oorzaken worden geassocieerd, en de gebeurtenis B stelt het effect voor.

We hernemen ons computervoorbeeld van hierboven. Veronderstel dat onze computer op een bepaald moment crasht omwille van een geheugenfout. Wat is de kans dat deze fout plaatsvond in een module van type 1?

We passen de regel van Bayes toe, en we bekomen

$$P(A_1 \mid B) = \frac{P(A_1)\,P(B \mid A_1)}{P(A_1)\,P(B \mid A_1) + P(A_2)\,P(B \mid A_2)}$$
$$= \frac{\frac{2}{3} \cdot 6 \cdot 10^{-18}}{\frac{2}{3} \cdot 6 \cdot 10^{-18} + \frac{1}{3} \cdot 3 \cdot 10^{-18}} = \frac{4 \cdot 10^{-18}}{5 \cdot 10^{-18}} = \frac{4}{5}\,.$$

De vals-positief paradox

We geven een ander voorbeeld dat gebruik maakt van de regel van Bayes, waarvan het resultaat zeer paradoxaal lijkt en tegen de intuïtie ingaat.

Van een test voor een bepaalde zeldzame ziekte wordt aangenomen dat hij in 95% van de gevallen correct is: indien een persoon die ziekte heeft, is het testresultaat met 0.95 kans positief, en als de persoon die ziekte niet heeft, is het testresultaat met 0.95 kans negatief. De ziekte komt gemiddeld bij 1 op 1 miljoen mensen voor. Als een willekeurig persoon positief test, wat is dan de kans dat hij die ziekte heeft?

Stel A de gebeurtenis dat die persoon de ziekte heeft, en B de gebeurtenis dat het testresultaat positief is. De gevraagde kans is dan $P(A \mid B)$, en de regel van Bayes geeft ons

$$P(A \mid B) = \frac{P(A)\,P(B \mid A)}{P(A)\,P(B \mid A) + P(A^{\mathrm{c}})\,P(B \mid A^{\mathrm{c}})}$$
$$= \frac{0.000001 \cdot 0.95}{0.000001 \cdot 0.95 + 0.999999 \cdot 0.05} \approx 0.000019\,.$$

Dus ondanks het feit dat de test zo accuraat lijkt, is de kans slechts 0.0019% dat een persoon die positief test, ook effectief deze ziekte heeft! De verklaring hiervoor ligt in het feit dat de 5% kans op een fout testresultaat bij personen die de ziekte niet hebben, veel zwaarder doorweegt dan de juiste testresultaten bij personen die de ziekte wel hebben, zodat het overgrote deel van de positieve testresultaten vals zijn.

Oefeningen

1. We trekken willekeurig 13 kaarten uit een volledig kaartspel van 52 kaarten. Als we weten dat we ten minste één aas getrokken hebben, wat is dan de kans dat we de vier azen getrokken hebben? En als we weten dat we schoppenaas getrokken hebben, wat is dan de kans dat we de vier azen getrokken hebben?

2. In een vaas zitten zes ballen: één zwarte, twee rode en drie gele. Als we zonder teruglegging één voor één drie ballen nemen uit de vaas, wat is dan de kans dat de eerste bal zwart is? En wat is de kans dat de tweede bal zwart is? En de derde?

3. Een examen bestaat uit waar-vals vragen. Als een student het antwoord weet op een vraag, dan antwoord hij ook correct; als hij het antwoord niet weet, dan gokt hij. Veronderstel dat een student op 60% van de vragen het antwoord kent. Als hij een bepaalde vraag correct heeft beantwoord, wat is dan de kans dat hij het antwoord gevonden heeft door te gokken?

3.4 Onafhankelijkheid van gebeurtenissen

Het begrip voorwaardelijke kans $P(A \mid B)$ werd ingevoerd om aan te geven in welke mate een gebeurtenis B informatie oplevert ten aanzien van een gebeurtenis A. Een interessant en belangrijk speciaal geval is dat waarbij B geen informatie oplevert en bijgevolg geen invloed heeft op de kans waarmee A optreedt, i.e. $P(A \mid B) = P(A)$.

We noemen een gebeurtenis A *stochastisch onafhankelijk*, of kortweg *onafhankelijk* van een gebeurtenis B, als

$$P(A \mid B) = P(A)\,,$$

of nog, als

$$P(A \cap B) = P(A)P(B)\,.$$

Indien $P(B) \neq 0$ volgt de equivalentie van deze twee voorwaarden uit de definitie van voorwaardelijke kans; in het geval dat $P(B) = 0$ hebben we aangenomen dat $P(A \mid B) = P(A)$, en dus zijn beide bovenstaande voorwaarden ook in dat geval equivalent (namelijk steeds allebei voldaan).

Merk op dat de tweede vorm symmetrisch is in A en B, zodat we onmiddellijk inzien dat A onafhankelijk is van B als en slechts als B onafhankelijk is van A. We zeggen dan ook eenvoudig dat A en B *onafhankelijke gebeurtenissen* zijn.

Stelling 3.4.1. *Als A en B onafhankelijk zijn, dan zijn A en B^{c} dat ook, evenals A^{c} en B^{c}.*

Bewijs. Omdat A en B onafhankelijk zijn, is $P(A \cap B) = P(A)P(B)$. Uit de totalekansformule halen we dan dat

$$P(A) = P(A \cap B) + P(A \cap B^{\mathrm{c}}) = P(A)P(B) + P(A \cap B^{\mathrm{c}})\,,$$

en dus is

$$P(A \cap B^{\mathrm{c}}) = P(A) - P(A)P(B) = P(A)(1 - P(B)) = P(A)P(B^{\mathrm{c}})\,;$$

hieruit volgt dat A en B^{c} onafhankelijk zijn. Door nu dezelfde redenering te herhalen op A zien we dat ook A^{c} en B^{c} onafhankelijk zijn. □

Onafhankelijkheid van gebeurtenissen is intuïtief vaak gemakkelijk te vatten, al kan het wel gebeuren dat twee gebeurtenissen die op het eerste gezicht afhankelijk van elkaar lijken, "bij toeval" toch onafhankelijk zijn.

Voorbeeld

Veronderstel dat we gooien met een blauwe en een rode vierzijdige dobbelsteen (die elk de waarden 1 tot en met 4 elk met een gelijke kans geven).

(a) Zijn de gebeurtenissen A "blauwe 2" en B "rode 3" onafhankelijk van elkaar? Intuïtief lijkt dit alvast zo, omdat de blauwe en rode dobbelsteen elkaar niet beïnvloeden tijdens het gooien. De berekeningen bevestigen dit: $P(A) = 1/4$, $P(B) = 1/4$, en $P(A \cap B) = 1/16$ omdat slechts 1 van de 16 mogelijke uitkomsten (die elk met gelijke kans voorkomen) aan beide voorwaarden voldoet; we zien dus dat $P(A \cap B) = P(A)P(B)$, en dus zijn A en B onafhankelijk van elkaar.

(b) Zijn de gebeurtenissen A "de hoogste waarde is een 2" en B "de laagste waarde is een 2" onafhankelijk van elkaar? Intuïtief verwachten we van niet, aangezien het minimum van de twee worpen partiële informatie geeft over het maximum. We gaan na dat $P(A) = 3/16$, $P(B) = 5/16$, en $P(A \cap B) = 1/16$, zodat inderdaad $P(A \cap B) \neq P(A)P(B)$, en de gebeurtenissen zijn afhankelijk van elkaar.

(c) Zijn de gebeurtenissen A "blauwe 2" en B "de som der ogen is 5" onafhankelijk van elkaar? Intuïtief verwachten we van niet, aangezien het resultaat van de ene dobbelsteen partiële informatie geeft over de som der ogen. Echter, we berekenen dat $P(A) = 1/4$, $P(B) = 1/4$, en $P(A \cap B) = 1/16$, zodat nochtans $P(A \cap B) = P(A)P(B)$, en dus zijn A en B toch onafhankelijk van elkaar. Dit is echter in zekere zin "toevallig", want als we de gebeurtenis B vervangen door "de som der ogen is 6", dan zijn A en B niet langer onafhankelijk van elkaar.

Voorwaardelijke onafhankelijkheid

Twee gebeurtenissen A en B worden *voorwaardelijk onafhankelijk* ten opzichte van een gebeurtenis C genoemd, als hun voorwaardelijke kans ten

opzichte van C onafhankelijk is, i.e. als

$$P(A \cap B \mid C) = P(A \mid C)\, P(B \mid C)\,.$$

Dit kan ook nog herschreven worden als

$$P(A \mid B \cap C) = P(A \mid C)\,;$$

dit betekent dus dat indien C zich heeft voorgedaan, de kennis van B de kans van A niet beïnvloedt.

Merk op dat de onvoorwaardelijke (on)afhankelijkheid van twee gebeurtenissen A en B niet hun voorwaardelijke (on)afhankelijkheid impliceert.

Als voorbeeld hiervan beschouwen we het experiment waarbij we twee vervalste muntstukken hebben. We hebben een blauw muntstuk, waarbij de kans op "kop" 0.99 is, en een rood muntstuk, waarbij de kans op "kop" 0.01 is. We kiezen willekeurig één van beide muntstukken en gooien het tweemaal achtereen op. Zij C de gebeurtenis "het blauwe muntstuk is geselecteerd", en zij K_1 en K_2 de gebeurtenissen om respectievelijk in de eerste en tweede beurt kop te gooien. Onder de voorwaarde C zijn de gebeurtenissen K_1 en K_2 onafhankelijk, want

$$P(K_1 \cap K_2 \mid B) = P(K_1 \mid B)\, P(K_2 \mid B) = 0.99 \cdot 0.99\,.$$

Echter, de gebeurtenissen K_1 en K_2 zijn niet onvoorwaardelijk onafhankelijk. Dit is reeds intuïtief duidelijk: als bekend is dat de eerste worp "kop" teruggaf, is de kans groot dat het blauwe muntstuk geselecteerd werd, in welk geval de kans dat ook de tweede worp "kop" teruggeeft, groot zal zijn. We rekenen dit na:

$$P(K_1) = P(B)\, P(K_1 \mid B) + P(B^{\mathrm{c}})\, P(K_1 \mid B^{\mathrm{c}}) = 0.5 \cdot 0.99 + 0.5 \cdot 0.01 = 0.5\,;$$

analoog is $P(K_2) = 0.5$. Echter,

$$\begin{aligned} P(K_1 \cap K_2) &= P(B)\, P(K_1 \cap K_2 \mid B) + P(B^{\mathrm{c}})\, P(K_1 \cap K_2 \mid B^{\mathrm{c}}) \\ &= 0.5 \cdot 0.99^2 + 0.5 \cdot 0.01^2 = 0.4901 \neq P(K_1)\, P(K_2)\,. \end{aligned}$$

Bijgevolg zijn K_1 en K_2 niet onafhankelijk van elkaar. Merk nog op dat de kans dat K_2 optreedt als we weten dat K_1 zich voordeed, inderdaad groot is:

$$P(K_2 \mid K_1) = \frac{P(K_1 \cap K_2)}{P(K_1)} = \frac{0.4901}{0.5} = 0.9802\,.$$

Onafhankelijkheid van een stel gebeurtenissen

De definitie van onafhankelijkheid van twee gebeurtenissen wordt als volgt veralgemeend voor het geval van meer dan twee gebeurtenissen. We noemen de gebeurtenissen $A_1, \ldots, A_n$ (onderling) *onafhankelijk* als

$$P\left(\bigcap_{i\in I} A_i\right) = \prod_{i\in I} P(A_i) \quad \text{voor alle } I \subseteq \{1,\ldots,n\}\,.$$

Merk op dat dit sterker is dan de *paarsgewijze* onafhankelijkheid van deze gebeurtenissen.

Beschouw bijvoorbeeld twee onafhankelijke worpen van een onvervalst muntstuk, en zij K_1 de gebeurtenis "kop bij de eerste worp", K_2 de gebeurtenis "kop bij de tweede worp", en V de gebeurtenis "de twee worpen tonen een verschillend resultaat". Merk op dat $P(K_1) = P(K_2) = P(V) = 1/2$. Anderzijds is $P(K_1 \cap K_2) = P(K_1 \cap V) = P(K_2 \cap V) = 1/4$, en dus zijn deze drie gebeurtenissen paarsgewijze onafhankelijk van elkaar. Echter, $P(K_1 \cap K_2 \cap V) = 0 \neq 1/8$, en dus zijn deze drie gebeurtenissen toch niet onderling onafhankelijk.

Ook omgekeerd volstaat de "sterkste" gelijkheid $P(A_1 \cap \cdots \cap A_n) = P(A_1)\cdots P(A_n)$ niet om de andere gelijkheden te besluiten. Beschouw daartoe bijvoorbeeld twee onafhankelijke worpen met een onvervalste dobbelsteen, en stel A gelijk aan de gebeurtenis "in de eerste beurt wordt een 1, 2 of 3 gegooid"; stel B gelijk aan de gebeurtenis "in de eerste beurt wordt een 3, 4 of 5 gegooid", en stel C gelijk aan de gebeurtenis "de som van de twee worpen is 9". Dan is

$$\begin{aligned} P(A\cap B) &= 1/6 \neq 1/2\cdot 1/2 = P(A)P(B)\,,\\ P(A\cap C) &= 1/36 \neq 1/2\cdot 1/9 = P(A)P(C)\,,\\ P(B\cap C) &= 1/12 \neq 1/2\cdot 1/9 = P(B)P(C)\,; \end{aligned}$$

anderzijds is nochtans

$$P(A\cap B\cap C) = 1/36 = 1/2\cdot 1/2\cdot 1/9 = P(A)P(B)P(C)\,.$$

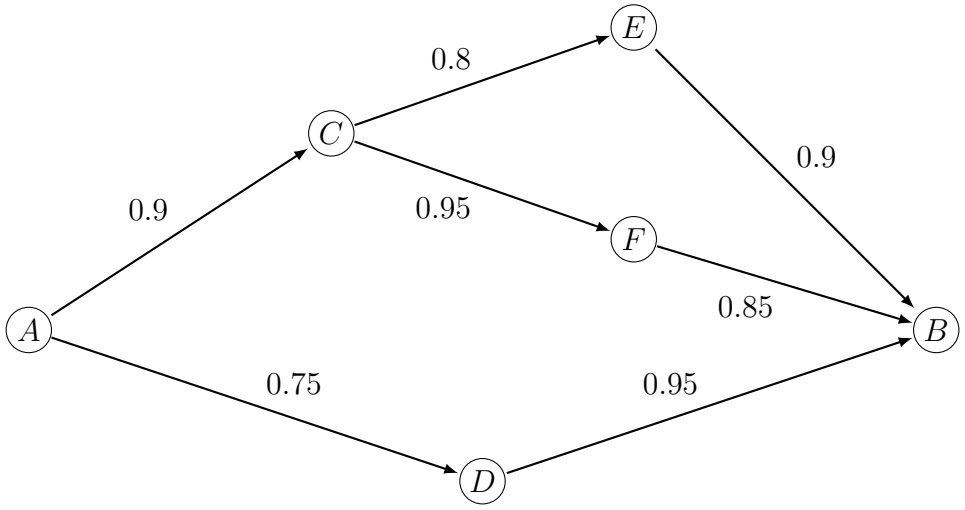
Oefeningen

1. We gooien een muntstuk drie keer na elkaar op. Beschouw de gebeurtenissen A om twee keer na elkaar kop te gooien, B om een even aantal keer kop te gooien, C dat we drie keer het zelfde resultaat gooien, en D dat we ten hoogste één keer munt gooien. Ga voor elk van de zes paren gebeurtenissen na of ze (paarsgewijze) onafhankelijk zijn van elkaar. Zijn de vier gebeurtenissen onderling onafhankelijk?

2. Zij E en F twee disjuncte gebeurtenissen, i.e. $E \cap F = \emptyset$. Zijn de gebeurtenissen E en F dan ook onafhankelijk van elkaar? Zo ja, waarom? Zo nee, wanneer zijn ze dat wel?

3.5 Betrouwbaarheid van netwerken

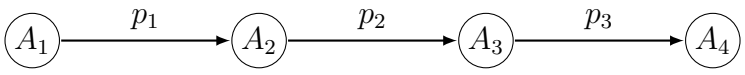
Als toepassing bespreken we de betrouwbaarheid van eenvoudige computernetwerken. Beschouw bijvoorbeeld het volgende netwerk, dat twee knooppunten A en B verbindt via intermediaire knopen C, D, E en F, zoals in onderstaande figuur. Hierbij geeft het getal bij elke verbinding weer wat de betrouwbaarheid van die verbinding is, i.e. de kans dat deze verbinding op een willekeurig moment probleemloos werkt. We veronderstellen ook dat de onderbrekingen in de verbindingen onafhankelijk van elkaar voorkomen.



Wat is de kans dat op een willekeurig moment de verbinding tussen A en B actief is?

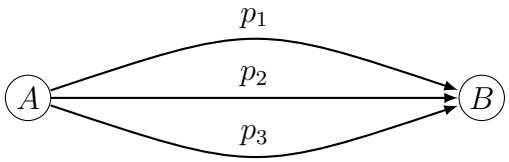
We kunnen een dergelijk systeem onderverdelen in subsystemen, waarbij elk subsysteem bestaat uit een aantal (grotere) componenten, die ofwel allemaal in serie, ofwel allemaal in parallel geschakeld zijn. We zullen dus eerst deze twee bijzondere gevallen bespreken.

Beschouw dus eerst een netwerk met $m + 1$ componenten $A_1, \ldots, A_{m+1}$ die via m verbindingen in serie staan, met respectieve betrouwbaarheid p_i.



Het is duidelijk dat de totale verbinding werkt als en slechts als elke deelverbinding werkt, en aangezien de betrouwbaarheid van de verbindingen onafhankelijk van elkaar ondersteld zijn, is de kans op een werkende totale verbinding gelijk aan $p_1 p_2 \cdots p_m$.

Beschouw vervolgens een netwerk met 2 componenten, die via m verbindingen in parallel staan, met respectieve betrouwbaarheid p_i.



Het is duidelijk dat de totale verbinding werkt als en slechts als ten minste één van de deelverbindingen werkt. Om deze kans te berekenen, is het eenvoudiger over te gaan naar de complementaire gebeurtenis "geen enkele deelverbinding werkt". Opnieuw omdat de betrouwbaarheid van de verbindingen onafhankelijk van elkaar ondersteld zijn, is de kans op deze gebeurtenis het product van de kans op falen van elk van de deelverbindingen, i.e. $(1-p_1)\cdots(1-p_m)$. De kans dat de totale verbinding werkt, is dan gelijk aan $1-(1-p_1)\cdots(1-p_m)$.

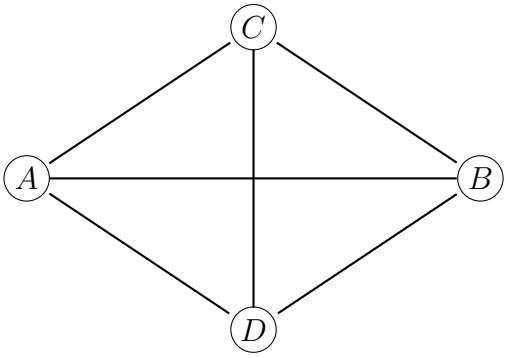
We passen dit nu toe op het voorbeeld. We zullen de kans dat de verbinding tussen knooppunt X en knooppunt Y actief is, noteren als p_{XY}. We bekomen dan achtereenvolgens dat

$$\begin{aligned} p_{CB} &= 1-\big(1-p_{CE}\cdot p_{EB}\big)\big(1-p_{CF}\cdot p_{FB}\big) \\ &= 1-\big(1-0.8\cdot 0.9\big)\big(1-0.95\cdot 0.85\big) = 0.9461\,; \end{aligned}$$

$$\begin{aligned} p_{AB} &= 1-\big(1-p_{AC}\cdot p_{CB}\big)\big(1-p_{AD}\cdot p_{DB}\big) \\ &= 1-\big(1-0.9\cdot 0.9461\big)\big(1-0.75\cdot 0.95\big) \approx 0.9573\,. \end{aligned}$$

Opmerking

Een complexer netwerk kan niet steeds "ontbonden" worden in serie- en parallelverbindingen, en voor dergelijke netwerken is onze methode ontoereikend. Beschouw bijvoorbeeld het volgend (ongericht) netwerk.



Er zal een verbinding zijn tussen de knooppunten A en B, als ten minste één van de paden A–B, A–C–B, A–D–B, A–C–D–B of A–D–C–B volledig in werking is. Om de uiteindelijke kans op een verbinding tussen A en B te bepalen, kan men bijvoorbeeld gebruik maken van het inclusie-exclusie principe, of men kan voor elk van de $2^6 = 64$ mogelijke situaties nagaan of de verbinding tussen A en B actief is, en de respectieve kansen op het voordoen van deze situaties optellen. We zullen deze (vrij lange) berekeningen hier niet uitvoeren.

3.6 Toevalsveranderlijken

3.6.1 Discrete toevalsveranderlijken

In veel probabilistische modellen zijn de uitkomsten numerieke waarden. Het is in die gevallen zinvol om aan deze waarden kansen te hechten en op die wijze een toevalsveranderlijke te construeren. Een *toevalsveranderlijke* (random variable) X over een uitkomstenverzameling S met probabiliteitsmaat P is een reëelwaardige functie van de uitkomsten in S, i.e. $X\colon S \to \mathbb{R}$.

Voorbeelden

(1) Als we een muntstuk vijf keer na elkaar opgooien, dan is het aantal keer dat we kop bekomen, een toevalsveranderlijke. De rij van de vijf uitkomsten is zelf géén toevalsveranderlijke, omdat deze rij geen reëel getal is.

(2) Als we twee dobbelstenen tegelijk gooien, dan is het totaal aantal ogen van de worp een toevalsveranderlijke. Ook het aantal zessen dat we gooien, of het product van de ogen van beide worpen, zijn voorbeelden van toevalsveranderlijken.

(3) Als we een bit-rij versturen over een netwerk, dan zijn de transmissietijd en het aantal bit-fouten voorbeelden van toevalsveranderlijken.

Een toevalsveranderlijke X is een *discrete toevalsveranderlijke* als de waardenverzameling $X(S)$ eindig of aftelbaar oneindig is.

Zo zijn de toevalsveranderlijken in voorbeeld (1) en (2) wel discreet, evenals het aantal bit-fouten in voorbeeld (3), maar de (exacte) transmissietijd in voorbeeld (3) is niet discreet. De transmissietijd afgerond op de milliseconde zou wel een discrete toevalsveranderlijke zijn.

Kansmassafunctie

Elke discrete toevalsveranderlijke X bezit een *kansmassafunctie* p_X, die de kansen weergeeft van de waarden die X kan aannemen:

$$p_X \colon X(S) \to [0,1] \colon x \mapsto P(X = x) := P\big(\{s \in S \mid X(s) = x\}\big)\,.$$

Met andere woorden, $p_X(x) = P(X = x)$ is de kans dat de toevalsveranderlijke X de waarde x aanneemt.

De kans dat een toevalsveranderlijke waarden aanneemt in een bepaalde vooropgegeven deelverzameling, kan eenvoudig worden bepaald uit de kansmassafunctie.

Stelling 3.6.1. *Zij X een discrete toevalsveranderlijke op een uitkomstenverzameling S. Dan geldt*

$$\sum_{x \in X(S)} p_X(x) = 1\,.$$

Algemener, als $T \subseteq X(S)$ een bepaalde deelverzameling van de waardenverzameling $X(S)$ is, dan geldt

$$P(X \in T) = \sum_{x \in T} p_X(x)\,.$$

Bewijs. De gebeurtenissen $\{X = x\}$ (met $x \in X(S)$) zijn disjunct, en vormen een partitie van de uitkomstenverzameling S als x alle mogelijke waarden van X doorloopt. Hieruit volgt onmiddellijk dat

$$1 = P(S) = P\left(\bigcup\nolimits_{x \in X(S)} \{X = x\}\right) = \sum_{x \in X(S)} P(X = x) = \sum_{x \in X(S)} p_X(x)\,.$$

Als T een deelverzameling is van $X(S)$, dan volgt geheel analoog dat

$$P(X \in T) = P\left(\bigcup\nolimits_{x \in T} \{X = x\}\right) = \sum_{x \in T} P(X = x) = \sum_{x \in T} p_X(x)\,. \qquad \square$$

Het is zeer gebruikelijk om de voorwaarde "$X \in T$" weer te geven door een concrete beschrijving, zoals bv. "$X > 2$", in plaats van expliciet de verzameling T te omschrijven.

Voorbeeld

Veronderstel dat we een onvervalst muntstuk twee keer opgooien, en stel X gelijk aan het aantal keren dat we kop gooien. Dan is X een toevalsveranderlijke op de uitkomstenverzameling $S = \{\text{KK}, \text{KM}, \text{MK}, \text{MM}\}$, en de kansmassafunctie is gegeven door

$$p_X(x) = \begin{cases} 1/4 & \text{als } x = 0 \text{ of } x = 2, \\ 1/2 & \text{als } x = 1, \\ 0 & \text{voor de overige } x. \end{cases}$$

De kans op ten minste één keer kop is gelijk aan

$$P(X \geq 1) = p_X(1) + p_X(2) = 1/2 + 1/4 = 3/4\,.$$

3.6.2 Bijzondere discrete toevalsveranderlijken

We vermelden een aantal vaak voorkomende toevalsveranderlijken.

Bernoulli-verdeelde toevalsveranderlijke

Beschouw één gooi van een muntstuk dat met kans p kop toont, en met kans $1 - p$ munt toont. De discrete toevalsveranderlijke X die de waarde 1 aanneemt als kop gegooid wordt, en 0 als munt gegooid wordt, is een *Bernoulli-verdeelde veranderlijke* of kortweg een *Bernoulli-veranderlijke*.

Een discrete toevalsveranderlijke X die Bernoulli-verdeeld is met parameter p, heeft de waardenverzameling $X(S) = \{0, 1\}$ en de kansmassafunctie

$$p_X(x) = \begin{cases} p & \text{als } x = 1, \\ 1 - p & \text{als } x = 0. \end{cases}$$

Bernoulli-veranderlijken worden dus gebruikt om probabilistische situaties met slechts twee mogelijke uitkomsten te modelleren.

Binomiaal verdeelde toevalsveranderlijke

Een muntstuk wordt n keer opgegooid. Bij elke gooi is p de kans op kop, en $1 - p$ de kans op munt, onafhankelijk van de vorige uitkomsten. Stel door

X het aantal keren kop in n gooien voor; dan is X een *binomiaal verdeelde toevalsveranderlijke* met parameters n en p (op de uitkomstenruimte S bestaande uit de mogelijke rijen van lengte n bestaande uit "kop" of "munt").

Een discrete toevalsveranderlijke X die binomiaal verdeeld is met parameters n en p, heeft de waardenverzameling $X(S) = \{0, 1, \ldots, n\}$ en de kansmassafunctie

$$p_X(k) = \binom{n}{k} p^k (1-p)^{n-k} \text{ voor } k = 0, \ldots, n$$

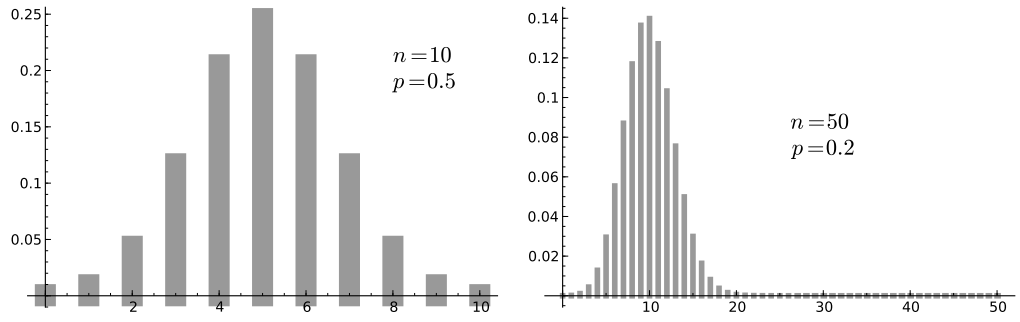
(en $p_X(k) = 0$ voor alle andere waarden van k).

Om in te zien dat het n keer opgooien van een muntstuk zoals beschreven, inderdaad een dergelijke kansmassafunctie heeft, volstaat het om in te zien dat er voor elke mogelijke uitkomst bestaande uit k keer "kop" en $n-k$ keer "munt" de kans om op te treden gelijk is aan $p^k(1-p)^{n-k}$, en dat er in de gehele uitkomstenverzameling precies $\binom{n}{k}$ uitkomsten zijn die k keer "kop" en $n-k$ keer "munt" vertonen. Het resultaat volgt dan uit Stelling 3.6.1.

In het bijzondere geval dat $n = 1$ vinden we een Bernoulli-verdeelde veranderlijke met parameter p terug. Merk op dat de som van de waarden die de kansmassafunctie kan aannemen, gelijk is aan 1, in overeenstemming met Stelling 3.6.1. Inderdaad, uit het binomium van Newton volgt dat

$$1 = \big(p + (1-p)\big)^n = \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} .$$

Dit verklaart tevens de naam van deze toevalsverdeling. Hieronder worden een paar voorbeelden van een binomiale verdeling geschetst. Merk op dat de kansmassafunctie symmetrisch is rond $x = n/2$ als $p = 1/2$, terwijl de verdeling naar links (resp. rechts) helt als $p < 1/2$ (resp. $p > 1/2$).



Geometrisch verdeelde toevalsveranderlijke

Een muntstuk waarvoor de kans om kop te gooien gelijk is aan p, wordt opgegooid tot een eerste keer kop wordt bekomen. De toevalsveranderlijke

die het aantal nodige gooien telt, is geometrisch verdeeld. Merk op dat de kans om voor het eerst kop te gooien in de k-de beurt gelijk is aan $(1-p)^{k-1}p$, zodat we komen tot de volgende definitie.

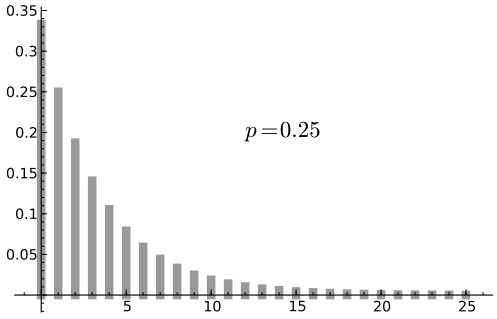
Een discrete toevalsveranderlijke X die geometrisch verdeeld is met parameter $p \in]0,1[$, heeft de waardenverzameling $X(S) = \{1, 2, \dots\}$ en de kansmassafunctie

$$p_X(k) = p(1-p)^{k-1} \text{ voor } k = 1, 2, \dots$$

(en $p_X(k) = 0$ voor alle andere waarden van k). Men verifieert gemakkelijk dat p_X een geldige kansmassafunctie is, aangezien

$$\sum_{k=1}^{\infty} p_X(k) = p \sum_{k=1}^{\infty} (1-p)^{k-1} = p \sum_{\ell=0}^{\infty} (1-p)^{\ell} = p \cdot \frac{1}{1-(1-p)} = 1\,.$$

De volgende figuur illustreert de kansmassafunctie van een geometrisch verdeelde toevalsveranderlijke.



3.6.3 Verwachtingswaarde en variantie

De kansmassafunctie p_X van een toevalsveranderlijke X is een verzameling van numerieke waarden, namelijk de kansen geassocieerd met de waarden die X kan aannemen. Het is wenselijk dat deze informatie zou samengevat worden in één of enkele representatieve getallen. De verwachtingswaarde en variantie van de toevalsveranderlijke X zijn dergelijke getallen.

Verwachtingswaarde

De verwachtingswaarde is een getal dat uitdrukt wat de gemiddelde uitkomst zal zijn van een bepaald experiment naarmate het aantal uitvoeringen van het experiment toeneemt. Het drukt dus uit wat men "gemiddeld gezien verwacht" als resultaat.

Beschouw bijvoorbeeld een kansspel met n mogelijke (positieve of negatieve) numerieke uitkomsten $m_1, \ldots, m_n$, die het gewonnen bedrag voorstellen, en die voorkomen met respectieve kansen gelijk aan $p_1, \ldots, p_n$. Wat is de verwachte winst per beurt?

Dit lijkt misschien een ietwat dubbelzinnige vraag, omdat in iedere beurt alle uitkomsten mogelijk zijn. Veronderstel echter dat het spel k keer gespeeld is, en stel door k_i het aantal keer voor dat m_i uitgekomen is. Dan is het totale gewonnen bedrag gelijk aan $m_1k_1 + \cdots + m_nk_n$, en dus is de gemiddelde winst per beurt gelijk aan

$$M = \frac{m_1k_1 + \cdots + m_nk_n}{k} = \frac{k_1}{k}\, m_1 + \cdots + \frac{k_n}{k}\, m_n\,.$$

Naarmate het aantal beurten k toeneemt, zullen de verhoudingen k_i/k naderen tot de bijhorende kans p_i; bijgevolg is de "verwachte" gemiddelde winst per beurt gelijk aan

$$p_1m_1 + \cdots + p_nm_n\,.$$

Dit inleidend voorbeeld motiveert de volgende definitie.

De *verwachtingswaarde* of *verwachting* (expected value) van een discrete toevalsveranderlijke X met kansmassafunctie p_X is gedefinieerd als

$$E[X] = \sum_{x \in X(S)} p_X(x)x\,.$$

Voorbeeld

We gooien drie keer met een vervalst muntstuk, dat kans $p = 1/3$ geeft om kop te gooien. Wat is het verwachte aantal keer dat we kop zullen gooien?

Oplossing.
Zij X de toevalsveranderlijke die het aantal keer kop telt; de bijhorende kansmassafunctie is

$$p_X(x) = \begin{cases} (2/3)^3 = 8/27 & \text{als } k = 0; \\ 3 \cdot (2/3)^2 \cdot (1/3)^1 = 4/9 & \text{als } k = 1; \\ 3 \cdot (2/3)^1 \cdot (1/3)^2 = 2/9 & \text{als } k = 2; \\ (1/3)^3 = 1/27 & \text{als } k = 3. \end{cases}$$

Bijgevolg is de verwachtingswaarde van X gelijk aan

$$E[X] = \frac{8}{27} \cdot 0 + \frac{4}{9} \cdot 1 + \frac{2}{9} \cdot 2 + \frac{1}{27} \cdot 3 = 1\,.$$

Dit komt overeen met onze intuïtie, en inderdaad, men kan ook algemeen aantonen dat indien X een binomiaal verdeelde toevalsveranderlijke is met parameters n en p, dat dan de verwachtingswaarde gelijk is aan

$$E[X] = np\,.$$

Functies van een discrete toevalsveranderlijke

We kunnen vanuit een discrete toevalsveranderlijke X andere discrete toevalsveranderlijken genereren door er een functie op los te laten; stel bijvoorbeeld

$$Y = g(X)$$

voor een zekere functie $g\colon \mathbb{R} \to \mathbb{R}$. Dan is ook Y opnieuw een discrete toevalsveranderlijke, en de kansmassafunctie van Y is gegeven door

$$p_Y(y) = \sum_{x \in X(S) | g(x) = y} p_X(x)\,.$$

Beschouw bijvoorbeeld een toevalsveranderlijke X met waardenverzameling $W = X(S) = \{-4, -3, \ldots, 3, 4\}$, en met kansmassafunctie

$$p_X(x) = \begin{cases} 1/9 & \text{als } x \in W; \\ 0 & \text{als } x \notin W. \end{cases}$$

Beschouw nu de toevalsveranderlijke $Y = X^2$; dan is de waardenverzameling van Y gelijk aan $\{0, 1, 4, 9, 16\}$, en de kansmassadichtheid p_Y is gegeven door

$$p_Y(y) = \begin{cases} 2/9 & \text{als } y \in \{1, 4, 9, 16\}; \\ 1/9 & \text{als } y = 0; \\ 0 & \text{anders.} \end{cases}$$

We kunnen de verwachtingswaarde van de toevalsveranderlijke $Y = g(X)$ eenvoudig rechtstreeks bepalen uit de functie g en de kansmassadichtheid van X.

Stelling 3.6.2 (Verwachtingswaarderegel voor functies van een discrete toevalsveranderlijke)**.** *Zij X een discrete toevalsveranderlijke met waardengebied W en kansmassafunctie p_X, en zij $g(X)$ een functie van X. De verwachtingswaarde van de toevalsveranderlijke $g(X)$ is dan gelijk aan*

$$E[g(X)] = \sum_{x \in W} p_X(x) g(x)\,.$$

Bewijs. Stel $Y = g(X)$. Dan is

$$\begin{aligned} E[g(X)] = E[Y] &= \sum_{y \in g(W)} p_Y(y) y = \sum_{y \in g(W)} \sum_{x \in W | g(x) = y} p_X(x) y \\ &= \sum_{y \in g(W)} \sum_{x \in W | g(x) = y} p_X(x) g(x) = \sum_{x \in W} p_X(x) g(x) \,. \end{aligned}$$ □

Momenten en variantie

Het *moment van k-de orde* of het *k-de moment* $\mu_k(X)$ van een toevalsveranderlijke X is de verwachtingswaarde van de toevalsveranderlijke X^k, i.e.

$$\mu_k(X) = E\big[X^k\big] \,.$$

De verwachtingswaarde is dus eveneens het moment van de eerste orde. Een andere belangrijke grootheid geassocieerd met een toevalsveranderlijke X is haar *variantie*, die genoteerd wordt als $\mathrm{var}(X)$ en gedefinieerd wordt als

$$\mathrm{var}(X) = E\big[(X - E[X])^2\big] \,.$$

De *standaardafwijking* (standard deviation) van een toevalsveranderlijke X is de toevalsveranderlijke σ_X gedefinieerd als

$$\sigma_X = \sqrt{\mathrm{var}(X)} \,.$$

Merk op dat de variantie nooit negatief is, aangezien $(X - E[X])^2$ uitsluitend niet-negatieve waarden aanneemt. De variantie is een maat voor de spreiding van X ten opzichte van de verwachtingswaarde; de standaardafwijking is een hiervan afgeleide spreidingsmaat die vaak eenvoudiger interpreteerbaar is omdat ze in dezelfde eenheden als X uitgedrukt wordt. (Bijvoorbeeld, als X een lengte uitdrukt in meter, dan is $\mathrm{var}(X)$ een grootheid in vierkante meter, en dan is σ_X opnieuw een grootheid in meter.)

Stelling 3.6.3. $\mathrm{var}(X) = E\big[X^2\big] - E[X]^2$.

Bewijs. We zullen gebruik maken van Stelling 3.6.2. Startend vanaf de definitie van $\mathrm{var}(X)$ krijgen we

$$\begin{aligned} \mathrm{var}(X) = E\big[(X - E[X])^2\big] &= \sum_x p_X(x) \big(x - E[X]\big)^2 \\ &= \sum_x p_X(x) \big(x^2 - 2xE[X] + E[X]^2\big) \\ &= \sum_x p_X(x) x^2 - 2E[X] \sum_x p_X(x) x + E[X]^2 \sum_x p_X(x) \\ &= E\big[X^2\big] - 2E[X]E[X] + E[X]^2 = E\big[X^2\big] - E[X]^2 \,. \end{aligned}$$ □

Voorbeeld

Beschouw opnieuw het voorbeeld waarbij we drie keer een vervalst muntstuk opgooien, dat met kans $p = 1/3$ kop teruggeeft. Dan is

$$E[X] = \frac{8}{27} \cdot 0 + \frac{4}{9} \cdot 1 + \frac{2}{9} \cdot 2 + \frac{1}{27} \cdot 3 = 1\,,$$

en

$$E\big[X^2\big] = \frac{8}{27} \cdot 0^2 + \frac{4}{9} \cdot 1^2 + \frac{2}{9} \cdot 2^2 + \frac{1}{27} \cdot 3^2 = 5/3\,.$$

De variantie is dus gelijk aan

$$\mathrm{var}(X) = E\big[X^2\big] - E[X]^2 = 5/3 - 1^2 = 2/3\,.$$

Men kan aantonen dat de variantie van een binomiaal verdeelde toevalsveranderlijke met parameters p en n gelijk is aan

$$\mathrm{var}(X) = np(1-p)\,.$$

Beslissen op grond van verwachtingswaarden

Verwachtingswaarden worden vaak aangewend in optimalisatieproblemen waarbij moet gekozen worden tussen verschillende opties die ieder een stochastische opbrengst genereren.

Beschouw bijvoorbeeld een quiz waarbij een kandidaat twee vragen krijgt en moet beslissen welk van beide vragen hij eerst wenst te beantwoorden. Stel dat vraag 1 met kans $p_1 = 0.8$ correct wordt beantwoord, en de kandidaat in dat geval $v_1 = 100$ euro ontvangt, terwijl vraag 2 met kans $p_2 = 0.5$ correct wordt beantwoord, en de kandidaat in dat geval $v_2 = 200$ euro ontvangt. Als hij de eerste vraag correct beantwoordt, mag hij ook de tweede vraag beantwoorden, maar indien hij de eerste vraag fout beantwoordt, is de quiz afgelopen en ontvangt hij niks. Welke vraag moet de kandidaat eerst beantwoorden om de opbrengst te maximaliseren?

Het antwoord is niet zonder meer duidelijk want er is een afweging te maken: starten met de moeilijkste maar meest winstgevende vraag geeft immers het risico dat de gemakkelijkere vraag niet eens meer mag beantwoord worden. Noem X de opbrengst; de oplossing bestaat erin om voor beide opties de verwachtingswaarde van X te berekenen, en de optie met de hoogste winstverwachting te kiezen.

(a) Veronderstel dat vraag 1 eerst wordt beantwoord. In dat geval is de kansmassafunctie van X gegeven door

$$p_X(0) = 0.2\,, \quad p_X(100) = 0.8 \cdot 0.5\,, \quad p_X(300) = 0.8 \cdot 0.5\,,$$

zodat de verwachte opbrengst gelijk is aan

$$E[X] = 0.2 \cdot 0 + 0.8 \cdot 0.5 \cdot 100 + 0.8 \cdot 0.5 \cdot 300 = 160\,.$$

(b) Veronderstel dat vraag 2 eerst wordt beantwoord. In dat geval is de kansmassafunctie van X gegeven door

$$p_X(0) = 0.5\,, \quad p_X(200) = 0.5 \cdot 0.2\,, \quad p_X(300) = 0.5 \cdot 0.8\,,$$

zodat de verwachte opbrengst gelijk is aan

$$E[X] = 0.5 \cdot 0 + 0.5 \cdot 0.2 \cdot 200 + 0.5 \cdot 0.8 \cdot 300 = 140\,.$$

Het is bijgevolg aangewezen om eerst de gemakkelijkere vraag te proberen.

Oefeningen

1. Beschouw de volgende procedure om het kleinste element te vinden in een array.

```
def FindMin(A,n):
    min = A[1]
    for i = 2 to n
        if A[i] < min
            min = A[i]
    return min
```

   Veronderstel dat de array A een willekeurige permutatie van de elementen van $\mathbb{N}[1, n]$ bevat. Wat is het verwachte aantal keren dat de waarde van `min` wordt overschreven tijdens het uitvoeren van de procedure?

2. Veronderstel dat we n items willen hashen in een hashtabel met k slots. Toon aan dat het verwachte aantal items dat in één welbepaalde slot terechtkomt, gelijk is aan n/k, in overeenstemming met wat je intuïtief zou verwachten.

3. Veronderstel dat we n items willen hashen in een hashtabel met k slots. Toon aan dat het verwachte aantal lege slots gelijk is aan $k(1 - 1/k)^n$, en dat het verwachte aantal collisions gelijk is aan $n - k + k(1 - 1/k)^n$.

4. Veronderstel dat we items willen hashen in een hashtabel met k slots. Toon aan dat het verwachte aantal items dat we nodig hebben om alle

slots te vullen, tussen $k \ln k + k/4$ en $k \ln k + k$ ligt. Maak hierbij gebruik van het feit dat

$$\frac{1}{4} + \ln k \leq \sum_{i=1}^{k} \frac{1}{i} \leq 1 + \ln k$$

voor alle $k \in \mathbb{N}^*$.

5. Veronderstel dat we n items willen hashen in een hashtabel met n slots. Dan is het verwachte aantal items in het vaakst gevulde slot van de grootte-orde $\log n / \log \log n$. Dit is heel wat moeilijker om aan te tonen, en je wordt dan ook niet verondersteld om dit zelf te kunnen.

Hoofdstuk 4

Voortbrengende functies

4.1 Formele machtreeksen

4.1.1 Inleiding

In paragraaf 2.10.2 hebben we als toepassing op de combinatieleer het binomium van Newton bewezen:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

of, in een enigszins aangepaste vorm

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Indien we de afspraak maken dat $\binom{n}{k}$ voor $k > n$ gelijk is aan nul, dan kunnen we dit binomium van Newton ook in de volgende vorm schrijven:

$$(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k.$$

De (oneindige) veelterm in x in het rechterlid wordt op die manier een *machtreeks in de onbepaalde variabele* x. Hierbij moeten we werkelijk x als een symbool interpreteren en niet als één of ander getal uit een getallenstructuur zoals in de cursus analyse gebeurt. We zullen ons dus ook niet moeten bekommeren om de convergentie van deze machtreeks. Daarom wordt een reeks

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

een *formele machtreeks* genoemd. De coëfficiënten a_k ($k \in \mathbb{N}$) behoren tot een bepaalde getallenverzameling, hier meestal tot $\mathbb{Z}$ of een deelverzameling van $\mathbb{Z}$.

Op die manier zal dus bij elke rij $(a_k)_{k\in\mathbb{N}}$ een formele machtreeks behoren. Omgekeerd bepalen de coëfficiënten van een formele machtreeks een rij getallen $(a_k)_{k\in\mathbb{N}}$.

Merk op dat elke veelterm

$$p(x) = \sum_{k=0}^{n} a_k x^k$$

steeds als een formele machtreeks geschreven kan worden, mits de afspraak dat $a_m = 0$ voor $m > n$.

Opmerking

Wij hebben hier angstvallig het woord *veeltermfunctie* vermeden omdat een functie (bijvoorbeeld van $\mathbb{R}$ naar $\mathbb{R}$) vastgelegd wordt door haar waarden, terwijl de reeksen die wij beschouwen vastgelegd worden door de *coëfficienten* a_n en door de *naam* van de onbepaalde variabele. Zo is bijvoorbeeld de functie

$$\begin{array}{rccl} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & a_0 + a_1 x + a_2 x^2 \end{array}$$

dezelfde als

$$\begin{array}{rccl} f: & \mathbb{R} & \to & \mathbb{R} \\ & x' & \mapsto & a_0 + a_1 x' + a_2 x'^2 \end{array}$$

terwijl de veeltermen $p(x) = a_0 + a_1 x + a_2 x^2$ en $p(x') = a_0 + a_1 x' + a_2 x'^2$ als veeltermen verschillend zijn.

4.1.2 Som en product van formele machtreeksen

Definities

De rekenregels voor de formele machtreeksen zijn nagenoeg dezelfde als deze voor de veeltermen. Zo zal de som en het product van formele machtreeksen op de volgende manier gedefinieerd worden.

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

Merk op dat de distributiviteitseigenschappen gelden voor deze optelling en vermenigvuldiging; meer bepaald krijgt de verzameling van formele machtreeksen in de variabele x op die manier de structuur van een *ring*; zie ook Hoofdstuk 8 verderop. We noteren deze ring als $\mathbb{R}[[x]]$.

Eén van de grote voordelen van formele machtreeksen (in vergelijking met veeltermen) is dat er veel meer inverteerbare elementen bestaan.

Stelling 4.1.1. *Als* $f(x) = \sum_{k=0}^{\infty} a_k x^k$ *en* $g(x) = \sum_{k=0}^{\infty} b_k x^k$ *twee formele machtreeksen zijn met* $b_0 \neq 0$*, dan bestaat er een unieke formele machtreeks* $h(x) = \sum_{k=0}^{\infty} c_k x^k$ *zodat* $f(x) = g(x) \cdot h(x)$*. We noteren* $h(x) = \frac{f(x)}{g(x)}$ *en noemen* $h(x)$ *het* quotiënt *van* $f(x)$ *en* $g(x)$*. Meer bepaald is*

$$h(x) = \frac{1}{b_0} \sum_{k=0}^{\infty} c_k x^k, \tag{4.1}$$

waarbij de coëfficiënten c_k *recursief gedefinieerd worden als* $c_0 = a_0$ *en*

$$c_k = a_k - \frac{1}{b_0} \sum_{i=1}^{k} b_i c_{k-i} \quad \textit{voor alle } k \geq 1.$$

Bewijs. We zullen rechtstreeks berekenen dat de formele machtreeks $h(x)$ zoals gedefinieerd in vergelijking (4.1) voldoet aan $g(x) \cdot h(x) = f(x)$. Uit bovenstaande formule voor het product van machtreeksen vinden we dat

$$\begin{aligned} g(x) \cdot h(x) &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} b_i \cdot \frac{1}{b_0} c_{k-i} \right) x^k \\ &= \sum_{k=0}^{\infty} \left(\frac{1}{b_0} \sum_{i=0}^{k} b_i c_{k-i} \right) x^k \\ &= \sum_{k=0}^{\infty} \left(c_k + \frac{1}{b_0} \sum_{i=1}^{k} b_i c_{k-i} \right) x^k \\ &= \sum_{k=0}^{\infty} a_k x^k = f(x). \end{aligned}$$

□

Toepassingen

We geven een aantal voorbeelden van bovenstaande stelling.

1. We kunnen bijvoorbeeld de volgende bewerkingen uitvoeren.

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

Aangezien nu x een onbepaalde variabele is, kunnen we schrijven dat

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k.$$

Vervangen we nu de onbepaalde variabele x door $-x$, dan ontstaat de betrekking

$$\begin{aligned}\frac{1}{1+x} &= \sum_{k=0}^{\infty} (-x)^k \\ &= 1 - x + x^2 - x^3 + x^4 - x^5 + \cdots .\end{aligned}$$

(We hadden deze uitdrukkingen ook kunnen berekenen met behulp van de formule (4.1).)

2. We zoeken een uitdrukking voor

$$\frac{1}{1-x-x^2}.$$

We passen hiervoor de formule (4.1) toe, met $f(x) = 1$ en $g(x) = 1 - x - x^2$. Merk op dat $a_i = 0$ voor alle $i \geq 1$ en dat $b_0 = 1$. We vinden dat

$$\frac{1}{1-x-x^2} = \sum_{k=0}^{\infty} c_k x^k,$$

met $c_0 = 1$ en

$$c_k = -\sum_{i=1}^{k} b_i c_{k-i}$$

voor alle $k \geq 1$. Voor $k = 1$ geeft dit $c_1 = -b_1 c_0 = 1$; voor $k \geq 2$ vinden we $c_k = c_{k-1} + c_{k-2}$. Uiteindelijk vinden we dus dat

$$\frac{1}{1-x-x^2} = 1 + x + 2x^2 + 3x^3 + 5x^4 + 8x^5 + \cdots$$

Merk terloops op dat

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

en dat de coëfficiënten van x in $1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots$ gelijk zijn aan $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$; deze getallen vormen een bekende rij, namelijk de rij van Fibonacci (zie pagina 107). We zullen dit verband later kunnen verklaren; zie Stelling 5.3.1 op p. 120.

3. Aangezien

$$(1-x^m)(1+x+x^2+\cdots)=1+x+x^2+\cdots+x^{m-1},\quad \forall m\in\mathbb{N}^*,$$

geldt

$$\sum_{i=0}^{\infty}x^i=\left(\sum_{k=0}^{m-1}x^k\right)(1-x^m)^{-1}\quad \forall m\in\mathbb{N}^*.$$

Indien

$$g(x)=\sum_{k=0}^{\infty}a_kx^k,$$

dan noemen we de formele machtreeks $\sum_{k=0}^{\infty}a_kx^k$ de *ontwikkeling* van $g(x)$.

Opmerking

In de vorige paragraaf hebben we een substitutie doorgevoerd door x te vervangen door $-x$. Willen we echter dit procédé algemeen toepassen, dan moeten we wel opletten.

Veronderstel dat we bijvoorbeeld in de machtreeks $\sum_{k=0}^{\infty}x^k$ de onbepaalde variabele vervangen door $1+x$. Dan verkrijgen we

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

Geen enkel van de coëfficiënten van machten van x in deze nieuwe reeks kan nog bepaald worden. Dit probleem zal zich niet voordoen indien we x vervangen door een formele machtreeks zonder constante term. We spreken dan ook in het vervolg af, dat we nooit substituties zullen uitvoeren waar x vervangen wordt door een machtreeks met een constante term verschillend van nul. Merk bovendien op dat we de onbepaalde variabele x niet zo maar mogen vervangen door een willekeurig getal, want dan komen we terug op het domein van de analyse, en moet er eerst een convergentie-onderzoek aan voorafgaan. Zo weten we bijvoorbeeld dat over de reële getallenverzameling $\mathbb{R}$, de reeks $\sum x^k$ enkel convergent is als $x\in]-1,+1[$.

4.1.3 Een andere kijk op het binomium van Newton

De theorie van de formele machtreeksen stelt ons in staat om een ander bewijs te geven van het binomium van Newton. Vooraleer we het bewijs presenteren, maken we de afspraak dat $\binom{n}{k}=0$ als $k>n$ of als $k<0$. Merk op dat door deze afspraak de formule van Stifel–Pascal (zie formule (2.1) op p. 33) geldt voor alle $k\in\mathbb{Z}$, ook als $k\leq 0$ of $k\geq n$.

Stelling 4.1.2. *Voor elke $n \in \mathbb{N}$ geldt*

$$(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k.$$

Bewijs. We geven het bewijs door gebruik te maken van volledige inductie; merk op dat de stelling triviaal waar is voor $n = 0$. Veronderstel nu dat

$$(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k.$$

Dan is

$$\begin{aligned}
(1+x)^{n+1} &= (1+x) \cdot (1+x)^n \\
&= (1+x) \cdot \sum_{k=0}^{\infty} \binom{n}{k} x^k \\
&= \sum_{k=0}^{\infty} \binom{n}{k} x^k + \sum_{k=0}^{\infty} \binom{n}{k} x^{k+1} \\
&= \sum_{k=0}^{\infty} \binom{n}{k} x^k + \sum_{k=1}^{\infty} \binom{n}{k-1} x^k \\
&= \sum_{k=0}^{\infty} \binom{n}{k} x^k + \sum_{k=0}^{\infty} \binom{n}{k-1} x^k \\
&= \sum_{k=0}^{\infty} \left(\binom{n}{k} + \binom{n}{k-1} \right) x^k = \sum_{k=0}^{\infty} \binom{n+1}{k} x^k.
\end{aligned}$$

□

Opmerking

Het voordeel van dit bewijs ligt in het feit dat we geen gebruik maken van combinatorische tellingen, maar enkel van de rekenregels in de ring $\mathbb{R}[[x]]$ van formele machtreeksen.

Toepassing

Indien we in het binomium van Newton voor $(1+t)^n$ de onbepaalde variabele t vervangen door $-x^m$ dan verkrijgen we de volgende uitdrukking:

$$(1-x^m)^n = 1 - \binom{n}{1} x^m + \binom{n}{2} x^{2m} - \cdots + (-1)^n x^{nm}.$$

4.2 Gewone voortbrengende functies

4.2.1 Definities

Veronderstel dat een rij $(a_k)_{k\in\mathbb{N}}$ gegeven wordt. Elke uitdrukking $g(x)$ waarvan de ontwikkeling gelijk is aan de formele machtreeks $\sum_{k=0}^{\infty} a_k x^k$, behorend bij de rij $(a_k)_{k\in\mathbb{N}}$, wordt een *(gewone) voortbrengende functie* (al is het geen functie) van deze rij genoemd. Soms zullen we de formele machtreeks zelf de voortbrengende functie noemen.

Voorbeelden

1. De voortbrengende functie van de rij $(1, -1, 1, -1, \ldots)$ is
$$(1+x)^{-1} = 1 - x + x^2 - x^3 + x^4 - x^5 + \cdots .$$
2. De voortbrengende functie van de rij $(1, 1, 1, 1, 1, \ldots)$ is
$$(1-x)^{-1} = 1 + x + x^2 + x^3 + x^4 + \cdots .$$
3. $(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k$ is de voortbrengende functie van de rij van de combinaties zonder herhaling van n elementen in groepen van k.

In de praktijk zullen de elementen van de rij $(a_k)_{k\in\mathbb{N}}$ het aantal oplossingen van een combinatorisch probleem (met andere woorden van één of andere telling) voorstellen. In het eerste hoofdstuk hebben we reeds heel wat telmethodes gezien. Soms zijn deze telmethodes zeer omslachtig of vragen ze veel rekenwerk. Zo komt het bij heel wat verdelingsproblemen voor, dat we een aantal elementen in groepjes willen splitsen waarbij we extra voorwaarden opleggen, bijvoorbeeld dat de groepjes minstens een aantal elementen van een bepaalde soort moeten bevatten, of dat elke groep een even aantal elementen moet bevatten. Dergelijke problemen zijn niet altijd eenvoudig op te lossen met de klassieke methodes. Hier komt de methode van de voortbrengende functies echter goed van pas.

Definitie

- Een *telprobleem* is een combinatorisch probleem met uitkomstenverzameling $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ (waarbij we toelaten dat bepaalde uitkomsten niet kunnen voorkomen), waarbij we geïnteresseerd zijn in het *aantal* keer dat elke uitkomst voorkomt.

- De *voortbrengende functie van een telprobleem* is de voortbrengende functie van de rij $(a_0, a_1, a_2, \dots)$, waarbij elke a_i gelijk is aan het aantal keer dat uitkomst i voorkomt; het is dus de formele machtreeks $\sum_{k=0}^{\infty} a_k x^k$.
- De *som van twee telproblemen* is het telprobleem waarbij we beide gegeven problemen naast elkaar uitvoeren, en dat als resultaat de som neemt van deze twee telproblemen. Zo is de som van "het aantal ogen bij het gooien met een dobbelsteen" en "het aantal ogen bij het gooien met een (andere) dobbelsteen" gelijk aan "het totaal aantal ogen bij het gooien van twee dobbelstenen".

De kracht van voortbrengende functies zit hem in de volgende stelling.

Stelling 4.2.1. *Beschouw twee telproblemen, met corresponderende voortbrengende functies gelijk aan* $f(x) = \sum_{k=0}^{\infty} a_k x^k$ *en* $g(x) = \sum_{k=0}^{\infty} b_k x^k$. *Dan is de voortbrengende functie van de som van deze twee telproblemen gelijk aan* $h(x) = f(x)g(x)$.

Bewijs. Zij $h(x) = \sum_{k=0}^{\infty} c_k x^k$ de voortbrengende functie van de som van de twee gegeven telproblemen. Voor elke $k \in \mathbb{N}$ is dan c_k gelijk aan het aantal keer dat de som van de twee problemen uitkomst k geeft. De mogelijke manieren om dit te verkrijgen, zijn:

- uitkomst 0 voor het eerste telprobleem en uitkomst k voor het tweede telprobleem;
- uitkomst 1 voor het eerste telprobleem en uitkomst $k-1$ voor het tweede telprobleem;
- uitkomst 2 voor het eerste telprobleem en uitkomst $k-2$ voor het tweede telprobleem;
- $\dots$
- uitkomst k voor het eerste telprobleem en uitkomst 0 voor het tweede telprobleem.

We zien dus dat

$$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i}.$$

Uit de definitie van het product van twee formele machtreeksen zien we dat dit precies betekent dat $h(x) = f(x)g(x)$. □

We zullen deze stelling aan de hand van enkele voorbeelden illustreren.

1. *Op hoeveel manieren kunnen we met twee dobbelstenen* 5 *ogen gooien?*

   Oplossing.

   Dit is een eenvoudig vraagstuk. We vragen eigenlijk op hoeveel manieren we 5 kunnen schrijven als een som van twee getallen uit $\mathbb{N}[1,6]$ (in feite zouden we ons kunnen beperken tot $\mathbb{N}[1,4]$). We kunnen dit probleem uiteraard eenvoudig oplossen zonder gebruik te maken van voortbrengende functies, maar we gebruiken dit eenvoudig voorbeeld om de nieuwe methode te illustreren. Met één dobbelsteen kunnen we $1, 2, 3, 4, 5$ of 6 gooien, en elk van deze mogelijkheden komt één keer voor. Deze informatie kunnen we opslaan in de rij

   $$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, \dots)$$

   of dus in de formele machtreeks

   $$f(x) = x + x^2 + x^3 + x^4 + x^5 + x^6 \, .$$

   Met de tweede dobbelsteen correspondeert eenzelfde machtreeks. Het aantal keren dat we met de twee dobbelstenen samen 5 ogen gooien, zullen we vinden als coëfficiënt van x^5 in het product van beide machtreeksen, dus in

   $$(x + x^2 + x^3 + x^4 + x^5 + x^6)^2.$$

   Alhoewel dit een eenvoudig vraagstuk was, kunnen we hieruit reeds een belangrijk voordeel op de klassieke methode opmerken. Inderdaad, we hebben hier een globale oplossing; we kunnen zonder meer de vraag beantwoorden voor elk aantal ogen gelegen tussen 1 en 12, want

   $$\begin{aligned}(x + x^2 + x^3 + x^4 + x^5 + x^6)^2 = {} & x^2 + 2x^3 + 3x^4 + 4x^5 + 5x^6 + 6x^7 \\ & + 5x^8 + 4x^9 + 3x^{10} + 2x^{11} + x^{12}.\end{aligned}$$

2. *Zoek het aantal drietallen* a, b, c *in* $\mathbb{N}[2,4]$ *waarvoor* $a + b + c = 10$.

   Oplossing.

   Aangezien er duidelijk niet zo veel oplossingen kunnen zijn voor dit

probleem, zullen we deze in een tabel onderbrengen.

a	b	c
2	4	4
4	2	4
4	4	2
3	3	4
3	4	3
4	3	3

Er zijn dus bijgevolg 6 oplossingen.

We willen dit probleem nu oplossen met behulp van voortbrengende functies; we "vertalen" het daarom eerst naar een telprobleem dat we kunnen zien als de som van drie andere (bijna triviale) telproblemen. Het eerste telprobleem correspondeert met de keuze van het getal a, en heeft als mogelijke uitkomsten enkel de waarden 2, 3, of 4, die elk één keer voorkomen. Hiermee correspondeert dus de formele machtreeks

$$p_a(x) = x^2 + x^3 + x^4 \,.$$

Hetzelfde geldt voor b en c. De veelterm $p(x) = p_a(x) \cdot p_b(x) \cdot p_c(x)$ is een veelterm van de graad 12 waarbij de laagst voorkomende macht van x gelijk is aan 6. Bovendien is de coëfficiënt van x_i gelijk aan het aantal oplossingen van $a + b + c = i$. Het probleem is op die manier herleid tot het bepalen van de coëfficiënt van x^{10} in $p(x) = (x^2 + x^3 + x^4)^3$ of van x^4 in $g(x) = (1 + x + x^2)^3$. Alhoewel de uitwerking van $g(x)$ in dit geval geen enkel probleem met zich meebrengt, zullen we gebruik maken van de multinomiaalstelling om de coëfficiënt te berekenen.

Volgens deze stelling is

$$\begin{aligned} g(x) &= (1 + x + x^2)^3 \\ &= \sum \binom{3}{(3 - n_1 - n_2), n_1, n_2} x^{n_1} (x^2)^{n_2} \,, \end{aligned}$$

waarbij de som genomen wordt over alle koppels (n_1, n_2) uit $\mathbb{N}[0, 3] \times \mathbb{N}[0, 3]$ zodanig dat $n_1 + n_2 \leq 3$. De coëfficiënt van x^4 in $g(x)$ is dus gelijk aan

$$\binom{3}{0, 2, 1} + \binom{3}{1, 0, 2} = \frac{3!}{0!\,2!\,1!} + \frac{3!}{1!\,0!\,2!} = 6 \,.$$

Merk op dat $p(x)$ de voortbrengende functie is van het aantal combinaties met herhaling van 3 elementen in groepen van k met de bijkomende

eigenschap dat elk element ten minste 2 maal en ten hoogste 4 maal voorkomt. Voor elke k vinden we dit aantal combinaties als coëfficiënt van x^k in $p(x)$. Uitgewerkt ziet $p(x)$ er als volgt uit:

$$p(x) = x^6 + 3x^7 + 6x^8 + 7x^9 + 6x^{10} + 3x^{11} + x^{12}.$$

Dit geeft ons dan ook een eerste voorbeeld van een combinatorisch probleem dat met de traditionele teltechnieken niet zo eenvoudig op te lossen is.

Zo zal de voortbrengende functie voor de combinaties van 4 letters, waarbij 1 letter tot 4 keer herhaald mag worden, een andere tot 2 keer toe en de overige 2 hoogstens 1 keer, gegeven worden door

$$(1 + x + x^2 + x^3 + x^4)(1 + x + x^2)(1 + x)(1 + x).$$

Het aantal manieren waarop men uit een verzameling knikkers van 3 verschillende kleuren, rood, groen en geel, er r kan uitnemen zodanig dat er ten hoogste 2 rode knikkers, ten hoogste 3 groene knikkers en ten hoogste 4 gele knikkers werden genomen, kan men vinden door de coëfficiënt van x^r te bepalen in de voortbrengende functie

$$g(x) = (1 + x + x^2)(1 + x + x^2 + x^3)(1 + x + x^2 + x^3 + x^4).$$

Of nog, de coëfficiënt van x^r in $g(x)$ is het aantal oplossingen in $\mathbb{N}$ van $a + b + c = r$, waarbij $a \leq 2,\ b \leq 3,\ c \leq 4$.

3. *Bepaal de voortbrengende functie $g(x)$ van de rij $(a_n)_{n\in\mathbb{N}}$, waarbij a_n het aantal oplossingen is in $\mathbb{N}$ van de vergelijking $2u + 3v + 5w = n$.*

Oplossing.

Aangezien $2u \in \{0, 2, 4, 6, \dots\}$, kunnen we hiermee de rij $(u_k)_{k\in\mathbb{N}} = (1, 0, 1, 0, 1, 0, \dots)$ laten corresponderen, zodat de bijhorende voortbrengende functie gelijk is aan $p_u(x) = (1+x^2+x^4+x^6+\cdots)$. Analoog zal $3v \in \{0, 3, 6, 9, \dots\}$ en $5w \in \{0, 5, 10, 15, \dots\}$, zodat de voortbrengende functies respectievelijk gelijk zijn aan $p_v(x) = (1+x^3+x^6+x^9+\cdots)$ en $p_w(x) = (1 + x^5 + x^{10} + \cdots)$. De voortbrengende functie van de rij $(a_n)_{n\in\mathbb{N}}$ is bijgevolg

$$\begin{aligned} g(x) &= p_u(x) \cdot p_v(x) \cdot p_w(x) \\ &= (1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots) \\ &\qquad \cdot (1 + x^5 + x^{10} + x^{15} + \cdots). \end{aligned}$$

4.2.2 De voortbrengende functie voor de herhalingscombinaties

Zoals gezegd is $(1+x)^n$ de gewone voortbrengende functie voor de combinaties zonder herhaling van n elementen. De volgende stelling geeft de voortbrengende functie van de combinaties met herhaling.

Stelling 4.2.2. *$(1-x)^{-n}$ is de voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ met*

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

Met andere woorden:

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

Bewijs. De voortbrengende functie die het aantal herhalingscombinaties weergeeft is

$$(1+x+x^2+x^3+\cdots)^n = \left(\frac{1}{1-x}\right)^n.$$

Inderdaad, de coëfficiënt van x^k geeft het aantal manieren waarop men x^k bekomt als product van n factoren van de vorm x^{k_i} met $\sum_{i=1}^{n} k_i = k$. Het is met andere woorden het aantal manieren waarop k geschreven kan worden als de som van n getallen uit $\mathbb{N}[0,k]$. Dit is de definitie (zie 2.9.4) van de herhalingscombinatie

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

We kunnen dus schrijven

$$\left(\frac{1}{1-x}\right)^n = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k. \qquad \square$$

Opmerking

Indien we rekening houden met de definitie van de binomiaalgetallen, dan kunnen we de coëfficiënt van x^k in de ontwikkeling van $(1-x)^{-n}$, $n \in \mathbb{N}^*$, als volgt omvormen.

$$\binom{n+k-1}{k} = \frac{(n+k-1)(n+k-2)\cdots(n+2)(n+1)n}{k!}$$

$$= \frac{(-1)^k\big((-n-k+1)(-n-k+2)\cdots(-n-2)(-n-1)(-n)\big)}{k!}$$
$$= (-1)^k \frac{(-n)(-n-1)\cdots(-n-(k-2))(-n-(k-1))}{k!}\,.$$

Bijgevolg, indien we nu de definitie van binomiaalgetallen formeel uitbreiden tot de negatieve gehele getallen $(-n)$ $(n \in \mathbb{N}^*)$

$$\binom{-n}{k} = \frac{(-n)(-n-1)\cdots(-n-(k-2))(-n-(k-1))}{k!},$$

dan volgt hieruit dat

$$\binom{n+k-1}{k} = (-1)^k \binom{-n}{k}.$$

Met deze definitie verkrijgen we voor de ontwikkeling van $(1-x)^{-n}$

$$(1-x)^{-n} = \sum_{k=0}^{\infty} \binom{-n}{k} (-1)^k x^k,$$

of indien we $-x$ vervangen door x,

$$(1+x)^{-n} = \sum_{k=0}^{\infty} \binom{-n}{k} x^k.$$

Bijgevolg mogen we hieruit besluiten, mits de uitbreiding van de definitie van de binomiaalgetallen $\binom{n}{k}$ voor gehele waarden van n, maar nog steeds $k \in \mathbb{N}$, dat

$$(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k.$$

Merk op dat de formule nog algemener kan gemaakt worden,

$$(a+b)^n = \sum_{k=0}^{\infty} \binom{n}{k} a^{n-k} b^k.$$

Men kan zelfs de binomiaalgetallen uitbreiden voor reële waarden van n, mits zogenaamde convergentievoorwaarden, maar dan zitten we echter op het terrein van de analyse.

Toepassing

Zoek het aantal oplossingen in $\mathbb{N}[3,8]$ *van de vergelijking* $a+b+c+d=27$.

Oplossing.
Het aantal oplossingen is de coëfficiënt van x^{27} in

$$g(x) = (x^3 + x^4 + \cdots + x^8)^4,$$

dit is ook de coëfficiënt van x^{15} in

$$h(x) = (1 + x + x^2 + \cdots + x^5)^4.$$

We hebben reeds vroeger gezien dat deze coëfficiënt door middel van de multinomiaalstelling kan worden gevonden. We geven hier een andere methode, die voor elk analoog vraagstuk toegepast kan worden.

Merk op dat

$$h(x) = (1 - x^6)^4(1 + x + x^2 + \cdots)^4.$$

Nu is

$$(1 - x^6)^4 = 1 - \binom{4}{1}x^6 + \binom{4}{2}x^{12} + \cdots,$$

(vervang hiervoor in het binomium van Newton voor $(1+t)^4$, de variabele t door $-x^6$). Anderzijds is (zie stelling 4.2.2)

$$(1 + x + x^2 + \cdots)^4 = 1 + \binom{4}{1}x + \binom{5}{2}x^2 + \binom{6}{3}x^3 + \cdots.$$

Bijgevolg is de coëfficiënt van x^{15} in $h(x)$ gelijk aan

$$\begin{aligned}\binom{18}{15} - \binom{4}{1}\binom{12}{9} + \binom{4}{2}\binom{6}{3} &= \frac{18!}{15!3!} - 4\frac{12!}{9!3!} + 6\frac{6!}{3!3!} \\ &= \frac{18\cdot 17\cdot 16}{6} - 4\frac{12\cdot 11\cdot 10}{6} + 6\frac{6\cdot 5\cdot 4}{6} \\ &= 816 - 880 + 120 \\ &= 56\,.\end{aligned}$$

De vergelijking $a+b+c+d=27$ bezit dus 56 oplossingen in $\mathbb{N}[3,8]$.

Oefeningen

1. Bepaal $g(x)$, zodanig dat $g(x)(1 + 2x + 3x^2 + 4x^3 + \cdots) = 1$.
2. Bepaal de coëfficiënt van x^7 in de ontwikkeling van $(1 + x + x^2)^{-1}$.
3. Bewijs dat voor alle natuurlijke getallen $k > 0$ geldt dat:

$$(-4)^{-k}\binom{2k}{k} = \binom{-\frac{1}{2}}{k}.$$

(gebruik inductie). Merk op dat

$$\binom{-\frac{1}{2}}{k} = \frac{\left(-\frac{1}{2}\right) \cdot \left(-\frac{1}{2} - 1\right) \cdots \left(-\frac{1}{2} - (k-1)\right)}{k!}.$$

4.2.3 Het aantal partities van een natuurlijk getal

Veronderstel dat we 4 gelijke knikkers bezitten, dan is het vlug in te zien dat er 5 verschillende manieren zijn om deze knikkers in porties te verdelen, namelijk gaande van 1 portie met 4 knikkers, 2 porties met resp. 3 en 1 knikker, 2 porties met elk 2 knikkers, 3 porties waarvan 1 met 2 knikkers en de andere 2 met elk 1 knikker tot tenslotte 4 porties met elk 1 knikker. Het zal duidelijk zijn dat voor grotere n deze aantallen vlug oplopen.

We noteren met p_n het aantal manieren waarop we een getal n in kleinere delen, verschillend van nul, kunnen verdelen. We noemen dit het *aantal partities* van n (niet te verwarren met de partities van een verzameling waar de elementen die tot een deelverzameling behoren mede bepalend zijn voor de partitie).

Zoals we zullen zien, is een eenvoudige formule voor de waarde van p_n moeilijk te geven. We kunnen wel de voortbrengende functie, behorend bij p_n opstellen.

Merk echter wel op dat het bepalen van p_n niet hetzelfde is als het bepalen van het aantal oplossingen van de vergelijking $x_1 + x_2 + \cdots + x_k = n$ voor alle mogelijke k met $1 \leq k \leq n$. Inderdaad, de oplossingen $x_1 = 2, x_2 = 3$ en $x_1 = 3, x_2 = 2$ zijn 2 verschillende oplossingen van de vergelijking $x_1 + x_2 = 5$, maar ze definiëren éénzelfde partitie van het getal 5.

Stelling 4.2.3. *Zij p_n het aantal partities van het getal n. Dan geldt*

$$\begin{aligned}\sum_{k=0}^{\infty} p_k x^k &= \prod_{i=1}^{\infty} \frac{1}{1 - x^i} \\ &= (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^3 + x^6 + \cdots) \cdots\end{aligned}$$

Bewijs. Als in een partitie van n het aantal delen van grootte i gelijk is aan x_i, dan geldt de volgende gelijkheid.

$$1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + \cdots + n \cdot x_n = n\,.$$

Mits de afspraak dat $x_i = 0$ als $i > n$ kunnen we dit ook schrijven als

$$\sum_{k=1}^{\infty} k x_k = n\,.$$

We proberen nu een formele machtreeks op te stellen voor het aantal oplossingen van deze vergelijking.

Als $x_1 = 0, 1, 2, 3, \ldots$ dan draagt de eerste term ook $0, 1, 2, 3, \ldots$ bij tot de som. Daarom geldt voor x_1 de formele machtreeks

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

Als $x_2 = 0, 1, 2, 3, \ldots$ dan draagt de tweede term $0, 2, 4, 6, \ldots$ bij tot de som. Daarom geldt voor x_2 de formele machtreeks

$$1 + x^2 + x^4 + x^6 + \cdots = \sum_{k=0}^{\infty} x^{2k} = \frac{1}{1-x^2}.$$

Op die manier geldt voor x_i de formele machtreeks

$$1 + x^i + x^{2i} + x^{3i} + \cdots = \sum_{k=0}^{\infty} x^{ik} = \frac{1}{1-x^i}.$$

Vermenigvuldigen we nu al deze machtreeksen met elkaar, dan resulteert dit in de machtreeks waarvan de coëfficiënt van x^n gelijk is aan het aantal partities p_n van n. □

Opmerking

Ter illustratie geven we hier een beperkte lijst van waarden van p_n. Het *efficiënt* berekenen van p_n (voor grote waarden van n) is overigens een zeer uitdagend probleem, waar bijzonder ingenieuze algoritmen voor ontwikkeld werden.

n	1	2	3	4	5	6	7	8	9	10	20	50	100
p_n	1	2	3	5	7	11	15	22	30	42	627	204226	190569292

4.3 Exponentieel voortbrengende functies

Het binomium van Newton leidt tot de gewone voortbrengende functie voor de rij van de combinaties (zowel met als zonder herhaling).

Merk nu echter op dat

$$\begin{aligned}(1+x)^n &= \sum_{k=0}^{\infty} \binom{n}{k} x^k \\ &= \sum_{k=0}^{\infty} \frac{V_n^k}{k!} x^k.\end{aligned}$$

In plaats van nu de formele machtreeksen met coëfficiënten a_k te gebruiken als voortbrengende functie van een rij $(a_k)_{k\in\mathbb{N}}$, kunnen we nu ook de formele machtreeksen met coëfficiënten $a_k/k!$ gebruiken. We spreken in dit geval van de *exponentieel voortbrengende functie*.

Met andere woorden, $g(x)$ is de exponentieel voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ dan en slechts dan als

$$g(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!}.$$

Bijgevolg is $(1+x)^n$ de exponentieel voortbrengende functie van de variaties van n elementen in groepen van k.

De exponentieel voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ gegeven door $a_k = 1$ voor alle $k \in \mathbb{N}$, is

$$\frac{1}{0!} + \frac{1}{1!}x^1 + \cdots + \frac{1}{k!}x^k + \cdots = \sum_{k=0}^{\infty} \frac{1}{k!} x^k.$$

Deze reeks is zeer gekend in de analyse. Inderdaad, indien we het als een functie over $\mathbb{R}$ opvatten, is het niets anders dan de reeksontwikkeling van de exponentiële functie e^x. Vandaar de naam: exponentieel voortbrengende functie. We definiëren dan ook de *formele exponentiële functie* e^x op de volgende manier:

$$e^x := \sum_{k=0}^{\infty} \frac{1}{k!} x^k.$$

Terloops gezegd, wie spreekt van exponentiële functie denkt onmiddellijk aan zijn inverse functie, met name de logaritmische functie $\ln(x)$. In analogie

met de reeksontwikkeling van $\ln(1+x)$, kunnen we hier de *formele logaritme* definiëren als

$$\ln(1+x) := x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \cdots + (-1)^{k+1}\frac{1}{k}x^k = \sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^k}{k}.$$

We kunnen niet genoeg herhalen dat de term "functie" slecht gekozen is, aangezien x ook hier een onbepaalde variabele is. Nochtans, de rekenregels die we kennen uit de analyse voor de logaritmische en de exponentiële functies, blijven ook hier geldig.

Net zoals de gewone voortbrengende functies hun nut bewijzen bij het beschouwen van de som van telproblemen, zo spelen de exponentieel voortbrengende functies een belangrijke rol bij het samenvoegen van geordende telproblemen.

Definitie

- Een *geordend telprobleem* is een combinatorisch probleem met als uitkomstenverzameling geordende rijen, waarbij we geïnteresseerd zijn in het *aantal* geordende rijen *van elke lengte* i.
- De *exponentieel voortbrengende functie van een geordend telprobleem* is de exponentieel voortbrengende functie van de rij $(a_0, a_1, a_2, \dots)$, waarbij elke a_i gelijk is aan het aantal geordende rijen van lengte i; het is dus de formele machtreeks $\sum_{k=0}^{\infty} a_k \frac{x^k}{k!}$.
- het *samenvoegen van twee geordende telproblemen* is het geordend telprobleem waarbij we beide gegeven problemen naast elkaar[1] uitvoeren, en vervolgens "in elkaar schuiven" op een willekeurige manier, d.w.z. dat de nieuwe rijen ontstaan door de rijen van beide problemen samen te voegen, zonder echter de onderlinge volgorde van de elementen van elk van de rijen te wijzigen. Zo is het samenvoegen van "woorden bestaande uit 4 of 5 letters" en "getallen bestaande uit 2 of 3 cijfers" gelijk aan "strings bestaande uit 4 of 5 letters en 2 of 3 cijfers".

De volgende stelling speelt een gelijkaardige rol als Stelling 4.2.1.

[1] We benadrukken dat we in de nieuwe rijen het onderscheid blijven maken tussen elementen afkomstig van het eerste probleem en elementen afkomstig van het tweede probleem, ook al zouden die toevallig op de zelfde manier neergeschreven worden.

Stelling 4.3.1. *Beschouw twee geordende telproblemen, met corresponderende exponentieel voortbrengende functies gelijk aan*

$$f(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!} \quad en \quad g(x) = \sum_{k=0}^{\infty} b_k \frac{x^k}{k!}\,.$$

Dan is de exponentieel voortbrengende functie van het samenvoegen van deze twee telproblemen gelijk aan $h(x) = f(x)g(x)$.

Bewijs. Zij $h(x) = \sum_{k=0}^{\infty} c_k \frac{x^k}{k!}$ de exponentieel voortbrengende functie van het samenvoegen van de twee gegeven geordende telproblemen. Voor elke $k \in \mathbb{N}$ is dan c_k gelijk aan het aantal geordende rijen van lengte k. De mogelijke manieren om dit te verkrijgen, zijn:

- het samenvoegen van een rij van lengte 0 uit het eerste probleem en een rij van lengte k uit het tweede probleem;
- het samenvoegen van een rij van lengte 1 uit het eerste probleem en een rij van lengte $k-1$ uit het tweede probleem;
- ...
- het samenvoegen van een rij van lengte k uit het eerste probleem en een rij van lengte 0 uit het tweede probleem.

Merk bovendien op dat het samenvoegen van een rij van lengte i uit het eerste probleem en een rij van lengte $k-i$ uit het tweede probleem op precies $\binom{k}{i}$ manieren kan. Bijgevolg is

$$c_k = \binom{k}{0} a_0 b_k + \binom{k}{1} a_1 b_{k-1} + \cdots + \binom{k}{k} a_k b_0 = \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}.$$

Anderzijds zien we dat het product $f(x)g(x)$ gelijk is aan

$$\begin{aligned} f(x)g(x) &= \left(\sum_{k=0}^{\infty} a_k \frac{x^k}{k!}\right) \cdot \left(\sum_{k=0}^{\infty} b_k \frac{x^k}{k!}\right) \\ &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} \frac{a_i}{i!} \cdot \frac{b_{k-i}}{(k-i)!}\right) x^k \\ &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} \frac{k!}{i!\,(k-i)!} \cdot a_i b_{k-i}\right) \frac{x^k}{k!} \\ &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}\right) \frac{x^k}{k!} = \sum_{k=0}^{\infty} c_k \frac{x^k}{k!} = h(x)\,. \end{aligned}$$

□

Voorbeelden

1. *Op hoeveel manieren kan men met de cijfers* 1, 2, 3 *getallen van* 5 *cijfers maken, zodanig dat elk getal ten minste* 3 *verschillende cijfers bevat?*

   Oplossing.

   Dit is in feite een rechtstreekse toepassing op de definitie van de multinomiaalgetallen. Inderdaad, het aantal getallen met 5 cijfers waarin het cijfer 1 en het cijfer 2 elk twee maal voorkomen (en dus het cijfer 3 één keer) is gelijk aan

   $$\frac{5!}{2!\,2!\,1!}.$$

   Het totaal aantal getallen dat aan de voorwaarden voldoet is gelijk aan

   $$\sum \frac{5!}{n_1!\,n_2!\,n_3!} \quad \text{met } n_i \in \mathbb{N}[1,3] \text{ en } n_1+n_2+n_3=5,$$

   en na enig rekenwerk vind je 150.

   We willen dit probleem nu oplossen door gebruik te maken van de exponentieel voortbrengende functies. Merk op dat in elk van de getallen een cijfer a ($a \in \{1,2,3\}$) één maal, twee maal of drie maal voorkomt. We kunnen het gegeven combinatorisch probleem dus zien als het samenvoegen van drie geordende telproblemen, waarbij elk van deze problemen met een ander cijfer overeenkomt. Zo heeft het geordend telprobleem dat met het cijfer 1 overeenkomt, slechts drie mogelijke uitkomsten, namelijk "1", "11" en "111"; we hebben dus één rij van elk van de lengtes 1, 2 of 3 (en geen rijen van andere lengtes). De overeenkomstige exponentieel voortbrengende functie is dus

   $$f(x) = x + \frac{x^2}{2!} + \frac{x^3}{3!}\,.$$

   De voortbrengende functie die bij het samenvoegen van deze drie geordende telproblemen hoort, is dan

   $$g(x) = \left(x + \frac{x^2}{2!} + \frac{x^3}{3!}\right)^3.$$

   Het aantal getallen met 5 cijfers zodanig dat elk van de cijfers 1, 2 of 3 ten minste één maal voorkomt is dan af te lezen als coëfficiënt van $x^5/5!$ in $g(x)$.

Een alternatieve manier om deze coëfficiënt te vinden gaat als volgt. Merk op dat de coëfficiënt van $x^5/5!$ niet wijzigt indien we als voortbrengende functie

$$g(x) = \left(\sum_{k=1}^{\infty} \frac{x^k}{k!} \right)^3$$

nemen. Nu is

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!},$$

zodat

$$g(x) = (e^x - 1)^3 = e^{3x} - 3e^{2x} + 3e^x - 1.$$

De coëfficiënt van $x^5/5!$ hierin, is uiteraard $3^5 - 3 \cdot 2^5 + 3 = 150$.

2. *We herhalen het vorige vraagstuk, waarbij we nu bovendien onderstellen dat de cijfers* 2 *en* 3 *elk ten hoogste* 2 *maal mogen voorkomen.*

   Oplossing.

   Het is duidelijk dat de bijhorende exponentieel voortbrengende functie er nu als volgt uitziet:

   $$g(x) = (e^x - 1) \left(x + \frac{x^2}{2!} \right)^2.$$

   Bepaal zelf de coëfficiënt van $x^5/5!$.

Oefeningen

1. Bewijs dat $(k!) \cdot S(n,k)$ de coëfficiënt is van $x^n/n!$ in $(e^x - 1)^k$. Hierbij is $S(n,k)$ het Stirling getal van de tweede soort (zie 2.11).

2. Bepaal de exponentieel voortbrengende functie die behoort bij het bepalen van het aantal woorden (zonder betekenis) die men kan maken met de letters van het woord MISSISSIPPI, waarbij elke letter ten hoogste zoveel keer mag voorkomen in de gemaakte woorden als in het woord MISSISSIPPI zelf.

3. Op hoeveel manieren kan men 9 personen plaatsen in 4 kamers, zodanig dat geen enkele kamer onbezet is?

4.4 De differentiaaloperator

We hebben reeds een formele definitie gegeven van som en product van formele machtreeksen. Deze definitie steunde op de rekenregels die we kennen voor veeltermfuncties. Op dezelfde manier, kunnen we op basis van de rekenregels voor de differentiaal van een veeltermfunctie, de *formele differentiaaloperator* D voor een formele machtreeks definiëren.

$$\begin{aligned} D(\sum_{n=0}^{\infty} a_n x^n) &:= \sum_{n=1}^{\infty} n a_n x^{n-1} \\ &= \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n \\ &= a_1 + 2a_2 x + 3a_3 x^2 + \cdots + (n+1)a_{n+1}x^n + \cdots . \end{aligned}$$

Als we de differentiatie $k \geq 1$ maal achter elkaar uitvoeren, dan krijgen we

$$\begin{aligned} D^k(\sum_{n=0}^{\infty} a_n x^n) &= k! a_k + \big((k+1)\cdots 2\big) a_{k+1} x + \big((k+2)\cdots 3\big) a_{k+2} x^2 + \cdots \\ &= \frac{k!}{0!} a_k + \frac{(k+1)!}{1!} a_{k+1} x + \frac{(k+2)!}{2!} a_{k+2} x^2 + \cdots \\ &= \sum_{n=k}^{\infty} \frac{n!}{(n-k)!} a_n x^{n-k} \\ &= \sum_{n=0}^{\infty} \frac{(n+k)!}{n!} a_{n+k} x^n. \end{aligned}$$

Deze formule is vooral belangrijk omdat men aan de constante term van de k-de differentiaal kan aflezen wat de coëfficiënt is van x^k in de oorspronkelijke machtreeks. De gebruikelijke rekenregels zoals de som–en productregel voor de differentiatie gelden ook hier.

$$\begin{aligned} D(f(x) + g(x)) &= D(f(x)) + D(g(x)) \\ D(f(x) \cdot g(x)) &= D(f(x)) \cdot g(x) + f(x) \cdot D(g(x)). \end{aligned}$$

Hieruit volgt onder andere dat voor alle $k > 0$,

$$D\big((g(x))^k\big) = k(g(x))^{k-1} D(g(x)).$$

Indien het quotiënt bestaat, dan geldt ook de traditionele quotiëntregel voor de differentiaal

$$D\left(\frac{f(x)}{g(x)}\right) = \frac{D(f(x))g(x) - f(x)D(g(x))}{(g(x))^2}.$$

Ten slotte mogen we ook de kettingregel voor de differentiaaloperator toepassen:

$$D(f(g(x))) = D_{g(x)}(f(g(x))) \cdot D(g(x)).$$

Hier bedoelen we met $D_{g(x)}$ de differentiaal waarbij $g(x)$ als variabele wordt beschouwd.

Het bewijs van al deze rekenregels laten we hier buiten beschouwing.

Oefeningen

1. Bewijs dat
   (a) $D(e^x) = e^x$.
   (b) $D(\ln(1+x)) = (1+x)^{-1}$.
2. Bereken $D\left((1+x)^n\right)$. Leid hieruit af dat

$$\sum_{k=0}^{n} k\binom{n}{k} = n \cdot 2^{n-1}.$$

4.5 Constructie van voortbrengende functies uit andere voortbrengende functies

Indien we één of meerdere voortbrengende functies kennen, dan hebben we gezien hoe we nieuwe voortbrengende functies kunnen construeren, door gebruik te maken van de som of het product van voortbrengende functies. Een ander voorbeeld is de voortbrengende functie $D(f(x))$ die ontstaat door de differentiaaloperator op $f(x)$ te laten inwerken.

In de volgende stelling worden enkele eigenschappen samengebracht. Het bewijs van deze stelling laten we als oefening.

Stelling 4.5.1. *Als $g(x)$ een voortbrengende functie is voor de rij $(a_k)_{k\in\mathbb{N}}$ en als $h(x)$ een voortbrengende functie is voor de rij $(b_k)_{k\in\mathbb{N}}$, dan gelden de volgende eigenschappen.*

(1) *$Ag(x) + Bh(x)$ is de voortbrengende functie voor $(Aa_k + Bb_k)_{k\in\mathbb{N}}$.*

(2) *$g(x)h(x)$ is de voortbrengende functie van $(a_0b_k + a_1b_{k-1} + \cdots + a_kb_0)_{k\in\mathbb{N}}$.*

(3) *$(1-x)g(x)$ is de voortbrengende functie voor $(a_k - a_{k-1})_{k\in\mathbb{N}^*}$ (waarbij we $a_{-1} = 0$ stellen).*

(4) $(1 + x + x^2 + \cdots)g(x) = \frac{g(x)}{1-x}$ *is de voortbrengende functie van de rij* $(a_0 + a_1 + \cdots a_k)_{k\in\mathbb{N}}$.

(5) $xD(g(x))$ *is de voortbrengende functie van* $(ka_k)_{k\in\mathbb{N}}$.

Voorbeelden

1. *Zoek de voortbrengende functie van de rij* $(a_k)_{k\in\mathbb{N}}$ *met* $a_k = 3k + 5k^2$.

   Oplossing.

   De voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ met $a_k = 1$ voor alle $k \in \mathbb{N}$ is

   $$g(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

   De voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ met $a_k = k$ voor alle $k \in \mathbb{N}$ is bijgevolg

   $$xD(g(x)) = \frac{x}{(1-x)^2}.$$

   De voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ met $a_k = k^2$ voor alle $k \in \mathbb{N}$ is anderzijds

   $$xD(xD(g(x))) = \frac{x + x^2}{(1-x)^3}.$$

   Hieruit volgt dus dat de voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ met $a_k = 3k + 5k^2$ gelijk is aan

   $$\begin{aligned} h(x) &= 3xD(g(x)) + 5xD(xD(g(x))) \\ &= \frac{3x}{(1-x)^2} + \frac{5x + 5x^2}{(1-x)^3} \\ &= \frac{3x(1-x) + 5x + 5x^2}{(1-x)^3} \\ &= \frac{8x + 2x^2}{(1-x)^3} \\ &= 2x\frac{x+4}{(1-x)^3}. \end{aligned}$$

   We vinden dus $a_k = 3k+5k^2$ als de coëfficiënt van x^k in de ontwikkeling van $2x(x + 4)(1 - x)^{-3}$.

Indien we omgekeerd zouden vertrekken van de voortbrengende functie

$$h(x) = 2x(x+4)(1-x)^{-3},$$

dan kunnen we de vormingswet van de coëfficiënten a_k in de ontwikkeling als volgt vinden.

Aangezien

$$f(x) = (1-x)^{-n}$$

de voortbrengende functie is van de rij $(a_k)_{k\in\mathbb{N}}$ met $a_k = \binom{k+n-1}{k}$, zal

$$(1-x)^{-3} = 1 + \binom{3}{1}x + \binom{4}{2}x^2 + \binom{5}{3}x^3 + \cdots + \binom{k+2}{k}x^k + \cdots .$$

Bijgevolg is

$$\begin{aligned} h(x) &= 2x(x+4)\left(\sum_{k=0}^{\infty}\binom{k+2}{k}x^k\right) \\ &= \sum_{k=0}^{\infty} 2\binom{k+2}{k}x^{k+2} + \sum_{k=0}^{\infty} 8\binom{k+2}{k}x^{k+1} \\ &= \sum_{k=2}^{\infty} 2\binom{k}{k-2}x^k + \sum_{k=1}^{\infty} 8\binom{k+1}{k-1}x^k \\ &= 8x + \sum_{k=2}^{\infty}\left(2\binom{k}{k-2} + 8\binom{k+1}{k-1}\right)x^k . \end{aligned}$$

Bijgevolg is $a_1 = 8$ en voor $k \geq 2$ is

$$\begin{aligned} a_k &= 2\binom{k}{k-2} + 8\binom{k+1}{k-1} \\ &= 2\frac{k(k-1)}{2} + 8\frac{k(k+1)}{2} \\ &= k(k-1) + 4k(k+1) \\ &= 3k + 5k^2. \end{aligned}$$

2. *Noteer V_n voor het totaal aantal variaties zonder herhaling die men kan maken met n elementen, m.a.w. $V_n = \sum_{k=0}^{n} V_n^k$. Bewijs dat $e^x(1-x)^{-1}$ de exponentieel voortbrengende functie is van de rij $(V_n)_{n\in\mathbb{N}}$.*

Oplossing.

We noemen $g(x)$ de exponentieel voortbrengende functie van de rij $(V_n)_{n\in\mathbb{N}}$:

$$g(x) = V_0 + V_1 x + \frac{V_2}{2!}x^2 + \cdots + \frac{V_n}{n!}x^n + \cdots .$$

We berekenen $g(x)(1-x)$.

$$\begin{aligned}
&g(x) - xg(x)\\
&= V_0 + (V_1 - V_0)\,x + \left(\frac{V_2}{2!} - V_1\right)x^2 + \cdots + \left(\frac{V_n}{n!} - \frac{V_{n-1}}{(n-1)!}\right)x^n + \cdots\\
&= V_0 + (V_1 - V_0)\,x + \left(\frac{V_2 - 2V_1}{2!}\right)x^2 + \cdots + \left(\frac{V_n - nV_{n-1}}{n!}\right)x^n + \cdots
\end{aligned}$$

Merk op dat $V_0 = 1$. Voor V_n, $n \geq 1$ geldt verder:

$$\begin{aligned}
V_n &= V_n^0 + V_n^1 + \cdots + V_n^{n-1} + V_n^n\\
&= 1 + n + n(n-1) + n(n-1)(n-2) + \cdots\\
&\qquad\qquad + n(n-1)(n-2)\cdots 2 + n!\\
&= 1 + n\Big(1 + (n-1) + (n-1)(n-2) + \cdots\\
&\qquad\qquad + (n-1)(n-2)\cdots 2 + (n-1)!\Big)\\
&= 1 + n \cdot V_{n-1}.
\end{aligned}$$

Met andere woorden:

$$V_n - n \cdot V_{n-1} = 1, \quad n \geq 1.$$

Bijgevolg is

$$\begin{aligned}
g(x) - xg(x) &= 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \cdots + \frac{1}{n!}x^n + \cdots\\
&= e^x.
\end{aligned}$$

Hoofdstuk 5

Recurrente betrekkingen

5.1 Definitie

Vaak wordt een rij $(a_n)_{n\in\mathbb{N}}$ op een *recursieve manier* gedefinieerd, m.a.w. door het opgeven van enkele specifieke waarden van a_i $(i = 0, \ldots, k-1)$ voor een zekere k en een vormingswet

$$a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k}), \quad n \geq k. \tag{5.1}$$

Dergelijke vormingswet wordt een *recurrente betrekking* voor de rij $(a_n)_{n\in\mathbb{N}}$ genoemd. Elke functie $g(n)$ zodanig dat de rij $a_n = g(n)$ voldoet aan (5.1), wordt een *oplossing* van de betrekking genoemd. Elke oplossing zal nog afhangen van de termen $a_0, a_1, \ldots, a_{k-1}$, die we de *vrijheidsgraden* van de recurrente betrekking noemen. Indien we geen specifieke waarden aan deze vrijheidsgraden geven, dan spreken we van de *algemene oplossing*. Indien we anderzijds aan alle vrijheidsgraden een specifieke waarde toekennen, dan spreken we van een *particuliere oplossing*.

Voorbeelden

- Het aantal wanordes d_n van $\mathbb{N}[1, n]$ voldoet aan de betrekking

$$d_n = (n-1)(d_{n-1} + d_{n-2}), \quad n \geq 3, \quad d_1 = 0, d_2 = 1.$$

- Indien we aannemen dat elk jaar de wereldbevolking met 3% toeneemt dan voldoet de omvang van de wereldbevolking aan de recurrente betrekking

$$a_n = 1.03 \cdot a_{n-1}, \quad n \geq 1.$$

- De rij van Fibonacci wordt gedefinieerd door

$$a_n = a_{n-1} + a_{n-2}, \quad n \geq 2, \quad a_0 = a_1 = 1.$$

  Deze rij is de oplossing van het gekende probleem, toegeschreven aan Fibonacci (bijnaam van Leonardo van Pisa (1180–1250)). Een konijnenpaar krijgt iedere maand een paar jongen. Ieder nieuw paar krijgt

vanaf de tweede maand ook weer steeds een paar jongen. Hoeveel konijnenparen zijn er aan het eind van iedere maand? De eerste tien termen uit deze rij zijn gelijk aan: $1, 1, 2, 3, 5, 8, 13, 21, 34, 55$.

Opmerking

Een algemene methode voor het oplossen van recurrente betrekkingen is moeilijk te geven. We zullen ons beperken tot de zogenaamde lineaire recurrente betrekkingen met constante coëfficiënten. In tegenstelling tot de recurrente betrekking voor het aantal wanordes van $\mathbb{N}[1, n]$, zijn de twee andere voorbeelden van een dergelijk type.

5.2 Lineaire recurrente betrekkingen met constante coëfficiënten

5.2.1 Definitie

Een *lineaire recurrente betrekking van de orde k met constante coëfficiënten* is een recurrente betrekking van de vorm

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + f(n), \quad n \geq k, \tag{5.2}$$

met $\lambda_1, \ldots, \lambda_k$ constanten. We veronderstellen bovendien dat $\lambda_k \neq 0$. Deze recurrente betrekking bezit k vrijheidsgraden $a_0, a_1, \ldots, a_{k-1}$. De recurrente betrekking wordt *homogeen* genoemd als $f(n) = 0$ voor alle $n \geq k$.

Stelling 5.2.1. *Indien $g_i(n)$ $(i = 1, 2, \ldots, m)$ oplossingen zijn van*

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + f_i(n), \quad n \geq k,$$

dan is elke lineaire combinatie $\sum_{i=1}^{m} \alpha_i g_i(n)$ $(\alpha_i \in \mathbb{R})$ van deze oplossingen een oplossing van de recurrente betrekking

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + \sum_{i=1}^{m} \alpha_i f_i(n), \quad n \geq k.$$

In het bijzonder is elke lineaire combinatie van oplossingen van een homogene recurrente betrekking terug een oplossing van deze betrekking.

Bewijs. Veronderstel dat

$$h(n) = \sum_{i=1}^{m} \alpha_i g_i(n).$$

Aangezien $g_i(n)$ oplossing is van

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + f_i(n), \quad n \geq k,$$

geldt

$$g_i(n) = \lambda_1 g_i(n-1) + \lambda_2 g_i(n-2) + \cdots + \lambda_k g_i(n-k) + f_i(n), \quad n \geq k,$$

zodat

$$\begin{aligned}
h(n) &= \sum_{i=1}^{m} \alpha_i g_i(n) \\
&= \sum_{i=1}^{m} \alpha_i \Big(\sum_{\ell=1}^{k} \lambda_\ell g_i(n-\ell) + f_i(n) \Big) \\
&= \sum_{i=1}^{m} \alpha_i \Big(\sum_{\ell=1}^{k} \lambda_\ell g_i(n-\ell) \Big) + \sum_{i=1}^{m} \alpha_i f_i(n) \\
&= \sum_{\ell=1}^{k} \lambda_\ell \Big(\sum_{i=1}^{m} \alpha_i g_i(n-\ell) \Big) + \sum_{i=1}^{m} \alpha_i f_i(n) \\
&= \sum_{\ell=1}^{k} \lambda_\ell h(n-\ell) + \sum_{i=1}^{m} \alpha_i f_i(n).
\end{aligned}$$

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

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + \sum_{i=1}^{m} \alpha_i f_i(n), \quad n \geq k. \qquad \square$$

5.2.2 Homogene lineaire recurrente betrekkingen met constante coëfficiënten

Er bestaat een vrij eenvoudige techniek om lineaire homogene recurrente betrekkingen op te lossen. Merk vooreerst op dat $a_n = r^n$ een oplossing is van de recurrente betrekking

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k}, \quad n \geq k, \tag{5.3}$$

dan en slechts dan als

$$r^n = \lambda_1 r^{n-1} + \lambda_2 r^{n-2} + \cdots + \lambda_k r^{n-k}, \quad n \geq k,$$

m.a.w. dan en slechts dan als ofwel $r = 0$ (maar dit leidt tot de triviale oplossing) ofwel r oplossing is van

$$x^k - \lambda_1 x^{k-1} - \lambda_2 x^{k-2} - \cdots - \lambda_{k-1} x - \lambda_k = 0. \tag{5.4}$$

Bijgevolg is de rij $(a_n)_{n\in\mathbb{N}}$ met $a_n = r^n$ een oplossing van (5.3), dan en slechts dan als r oplossing is van (5.4). We noemen de vergelijking (5.4) de *karakteristieke vergelijking* van de recurrente betrekking (5.3). De oplossingen van deze karakteristieke vergelijking worden de *karakteristieke oplossingen* van de recurrente betrekking (5.3) genoemd. Zoals we zullen zien, kunnen de karakteristieke oplossingen gebruikt worden om een expliciete formule voor de oplossingen van de recurrente betrekking op te stellen. We zullen eerst de homogene lineaire recurrente betrekkingen van orde 1 en 2 bespreken.

Homogene lineaire recurrente betrekkingen van eerste orde

We zoeken de oplossingen van de recurrente betrekking van de vorm

$$a_n = ca_{n-1}, \quad n \geq 1. \tag{5.5}$$

De karakteristieke vergelijking die hierbij behoort is $(x - c) = 0$. Bijgevolg is de algemene oplossing van de homogene lineaire recurrente betrekking van de eerste orde $a_n = ca_{n-1}$ van de vorm $a_n = \alpha c^n$. Merk op dat $a_0 = \alpha c^0 = \alpha$ zodat de rij volledig bepaald is indien de waarde van a_0 gekend is. De algemene oplossing van de homogene lineaire recurrente betrekking (5.5) is bijgevolg gelijk aan $a_n = c^n a_0$. Een rij $(a_n)_{n\in\mathbb{N}}$ met $a_n = c^n a_0$ wordt een *meetkundige rij met reden c* genoemd.

Homogene lineaire recurrente betrekkingen van tweede orde

De karakteristieke vergelijking die behoort bij de homogene lineaire recurrente betrekking van tweede orde

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2}, \quad n \geq 2, \tag{5.6}$$

is

$$x^2 - \lambda_1 x - \lambda_2 = 0. \tag{5.7}$$

Het oplossen van homogene lineaire recurrente betrekkingen van tweede orde is met andere woorden herleid tot het oplossen van een kwadratische vergelijking.

Veronderstel eerst dat (5.7) twee verschillende (eventueel complex toegevoegde) oplossingen heeft, stel r_1 en r_2. Dan zijn zowel $a_n = r_1^n$ als $a_n = r_2^n$ oplossingen van (5.6), en uit Stelling 5.2.1 volgt dan dat

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n \tag{5.8}$$

een oplossing is van (5.6), voor elke mogelijke waarde van α_1 en van α_2.

We beweren nu dat *elke* oplossing van (5.6) van deze vorm is. Inderdaad, veronderstel dat de beginwaarden $a_0 = k_0$ en $a_1 = k_1$ gegeven zijn, en beschouw het stelsel

$$\begin{cases} k_0 = \alpha_1 + \alpha_2 \\ k_1 = \alpha_1 r_1 + \alpha_2 r_2. \end{cases}$$

De determinant van het stelsel is gelijk aan $r_2 - r_1$ en dus verschillend van nul, zodat er juist één oplossing α_1 en α_2 kan gevonden worden. Voor deze waarden van α_1 en α_2 geeft (5.8) de unieke particuliere oplossing van (5.6) die aan de gegeven beginvoorwaarden voldoet. We besluiten dus dat de *algemene* oplossing van (5.6) gegeven wordt door (5.8).

Veronderstel nu dat (5.7) een unieke oplossing heeft, m.a.w. dat de discriminant van (5.7) gelijk is aan nul. Dan is (5.7) gelijkwaardig met

$$\left(x - \frac{\lambda_1}{2}\right)^2 = 0,$$

zodat deze unieke oplossing van (5.7) gelijk is aan $r = \lambda_1/2$. (Merk op dat $r \neq 0$ omdat anders $c_1 = c_2 = 0$ zou zijn.) Bijgevolg is $a_n = (\lambda_1/2)^n$ een oplossing van de recurrente betrekking (5.6). In dit geval is echter $a_n = nr^n = n(\lambda_1/2)^n$ eveneens oplossing van (5.6) (bewijs als oefening). Uit Stelling 5.2.1 volgt nu opnieuw dat

$$a_n = (\alpha_1 + \alpha_2 n) r^n \tag{5.9}$$

een oplossing is van (5.6), voor elke mogelijke waarde van α_1 en van α_2.

Ook hier beweren we dat *elke* oplossing van (5.6) van deze vorm is. Inderdaad, veronderstel dat de beginwaarden $a_0 = k_0$ en $a_1 = k_1$ gegeven zijn, en beschouw het stelsel

$$\begin{cases} k_0 = \alpha_1 \\ k_1 = (\alpha_1 + \alpha_2) r. \end{cases}$$

Het is duidelijk dat dit stelsel een unieke oplossing (α_1, α_2) heeft. Voor deze waarden van α_1 en α_2 geeft (5.9) de unieke particuliere oplossing van (5.6) die aan de gegeven beginvoorwaarden voldoet. We besluiten dus dat de *algemene* oplossing van (5.6) gegeven wordt door (5.9).

Homogene lineaire recurrente betrekkingen van hogere orde

De techniek voor de homogene lineaire recurrente betrekkingen van eerste en tweede orde kan zonder meer uitgebreid worden tot hogere orden. We vatten deze techniek samen in de volgende stelling.

Stelling 5.2.2. *Als de wortels $r_1, r_2, \ldots, r_k$ van de karakteristieke vergelijking behorend bij de recurrente betrekking*

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k}$$

allemaal verschillend zijn, dan is de algemene oplossing

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n,$$

met $\alpha_1, \ldots, \alpha_k$ willekeurige getallen. Als r een wortel is van de karakteristieke vergelijking met multipliciteit m, dan is

$$(\alpha_0 + \alpha_1 n + \alpha_2 n^2 + \cdots + \alpha_{m-1} n^{m-1}) r^n$$

een oplossing van de recurrente betrekking, voor willekeurige waarden van $\alpha_0, \ldots, \alpha_{m-1}$.

Zonder bewijs. □

Voorbeelden

1. *Bepaal een algemene term uit de rij $(a_n)_{n\in\mathbb{N}}$ gedefinieerd door $a_0 = 1$, $a_1 = 5$ en $a_n = 5a_{n-1} - 6a_{n-2},\ n \geq 2$.*

   Oplossing.

   De karakteristieke vergelijking die bij deze homogene lineaire recurrente betrekking van de tweede orde behoort, is

   $$x^2 - 5x + 6 = 0.$$

   Een algemene oplossing is bijgevolg

   $$a_n = \alpha_1 \cdot 2^n + \alpha_2 \cdot 3^n. \tag{5.10}$$

   Aangezien $a_0 = 1$ en $a_1 = 5$ geldt

   $$\begin{cases} \alpha_1 + \alpha_2 = 1 \\ 2\alpha_1 + 3\alpha_2 = 5. \end{cases}$$

   Bijgevolg is $\alpha_1 = -2$ en $\alpha_2 = 3$. De algemene term a_n is bijgevolg gelijk aan $3^{n+1} - 2^{n+1}$.

2. *Bepaal een algemene term uit de rij van Fibonacci.*

Oplossing.

De karakteristieke vergelijking die behoort bij de rij van Fibonacci is $x^2 - x - 1 = 0$. Deze vergelijking bezit 2 verschillende oplossingen

$$r_1 = \frac{1+\sqrt{5}}{2} \quad \text{en} \quad r_2 = \frac{1-\sqrt{5}}{2}.$$

De algemene oplossing is bijgevolg

$$a_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Aangezien $a_0 = a_1 = 1$, geldt

$$\begin{cases} \alpha_1 + \alpha_2 = 1 \\ \left(\frac{1+\sqrt{5}}{2}\right)\alpha_1 + \left(\frac{1-\sqrt{5}}{2}\right)\alpha_2 = 1. \end{cases}$$

Hieruit volgt dat

$$\alpha_1 = \frac{1}{2} + \frac{\sqrt{5}}{10}$$
$$\alpha_2 = \frac{1}{2} - \frac{\sqrt{5}}{10}.$$

De algemene term uit de rij van Fibonacci is bijgevolg

$$a_n = \left(\frac{1}{2} + \frac{\sqrt{5}}{10}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1}{2} - \frac{\sqrt{5}}{10}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

3. *Los volgende recurrente betrekking op:* $a_n = 6a_{n-1} - 9a_{n-2}$, $n \geq 2$. *Zoek tevens de particuliere oplossing als de beginvoorwaarden* $a_0 = 1$ *en* $a_1 = 2$ *gegeven zijn.*

Oplossing.

De bijhorende karakteristieke vergelijking is $x^2 - 6x + 9 = 0$ en heeft dus een wortel $x = 3$ met multipliciteit 2. Bijgevolg is de algemene oplossing van deze recurrente betrekking

$$a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot n \cdot 3^n.$$

In de veronderstelling dat bovendien $a_0 = 1$ en $a_1 = 2$, volgt hieruit dat $\alpha_1 = 1$ en $\alpha_2 = -1/3$, zodat met deze beginvoorwaarden, de particuliere oplossing van de recurrente betrekking gegeven wordt door

$$a_n = 3^n - n \cdot 3^{n-1}.$$

4. *Zoek de oplossing van de recurrente betrekking*

$$a_n = 3a_{n-1} + 6a_{n-2} - 28a_{n-3} + 24a_{n-4}, \quad n \geq 4,$$

die voldoet aan de voorwaarden $a_0 = 8,\ a_1 = -5,\ a_2 = 81,\ a_3 = -15.$

Oplossing.

De karakteristieke vergelijking die hierbij behoort, is

$$x^4 - 3x^3 - 6x^2 + 28x - 24 = 0.$$

Deze vergelijking bezit een drievoudige wortel 2 en een enkelvoudige wortel -3. De algemene oplossing is derhalve:

$$a_n = (\alpha_0 + \alpha_1 n + \alpha_2 n^2)2^n + \alpha_3(-3)^n.$$

De beginvoorwaarden leveren de waarden van de coëfficiënten, en men bekomt na enig rekenwerk:

$$a_n = (n^2 + n + 3)2^n + 5(-3)^n.$$

Oefeningen

Los volgende recurrente betrekkingen op:

1. $2a_n - 3a_{n-1} - 2a_{n-2} = 0,\ n \geq 2,\ a_0 = 0,\ a_1 = -5.$
2. $4a_n - 12a_{n-1} + 9a_{n-2} = 0,\ n \geq 2,\ a_0 = 2,\ a_1 = 3/2.$
3. $a_n = 8(a_{n-1} - 2a_{n-2}),\ n \geq 2,\ a_0 = 1,\ a_1 = 5.$
4. $a_n = 2a_{n-2} - a_{n-4},\ n \geq 4,\ a_0 = 2,\ a_1 = a_3 = 0,\ a_2 = 6.$

De matrixmethode voor homogene lineaire betrekkingen van hogere orde

Een theoretisch interessante manier om homogene lineaire recurrente betrekkingen met constante coëfficiënten van tweede en hogere orde aan te pakken, is deze te herleiden tot een stelsel van recurrente betrekkingen van eerste orde. Dit gaat als volgt. In plaats van getallen a_n te zoeken die aan een betrekking

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k}, \quad n \geq k,$$

voldoen, schakelen we over op *kolommatrices* met k rijen:

$$\mathcal{A}_{n-1} := \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ \vdots \\ a_{n-k} \end{pmatrix}.$$

Het verband tussen de kolommatrices $\mathcal{A}_n$ en $\mathcal{A}_{n-1}$ kan dan door de volgende matrixvergelijking beschreven worden.

$$\begin{pmatrix} a_n \\ a_{n-1} \\ a_{n-2} \\ \vdots \\ a_{n-k+1} \end{pmatrix} = \begin{pmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \cdots & \lambda_{k-1} & \lambda_k \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} . \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ a_{n-3} \\ \vdots \\ a_{n-k} \end{pmatrix}.$$

Dit kunnen we kort schrijven als

$$\mathcal{A}_n = \mathcal{C} \cdot \mathcal{A}_{n-1}.$$

Hierbij is de $k \times k$ matrix $\mathcal{C}$ in de bovenstaande matrixvergelijking volledig bepaald door de gegeven recurrente betrekking. Door achtereenvolgende substitutie bekomen we het stelsel

$$\mathcal{A}_n = \mathcal{C}^{n-k+1} \cdot \mathcal{A}_{k-1}.$$

De kolommatrix

$$\mathcal{A}_{k-1} = \begin{pmatrix} a_{k-1} \\ a_{k-2} \\ \vdots \\ a_0 \end{pmatrix},$$

is de matrix van de k vrijheidsgraden. Het probleem is op die manier herleid tot een probleem van de lineaire algebra (product van matrices).

Voorbeeld

Bij wijze van voorbeeld passen we de matrixmethode toe op de Fibonaccigetallen. De recurrente betrekking is van de tweede orde $a_n = a_{n-1} + a_{n-2}$, en wordt dus herleid tot het oplossen van een 2×2 stelsel:

$$\begin{pmatrix} a_n \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} \\ a_{n-2} \end{pmatrix}.$$

Bijgevolg geldt

$$\begin{pmatrix} a_n \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} a_1 \\ a_0 \end{pmatrix}.$$

De Fibonaccigetallen volgen dan uit deze matrixvergelijking waarbij $a_0 = a_1 = 1$. We merken terloops op dat men soms ook wel als beginvoorwaarden voor de rij van Fibonacci $a_0 = 0$ en $a_1 = 1$ neemt. Er worden ook andere beginvoorwaarden gebruikt, zoals bijvoorbeeld $a_0 = 2$ en $a_1 = 1$, in dit geval wordt de rij meestal de Lucasrij genoemd (naar de Franse wiskundige François Lucas (1842–1891) die in feite het konijnenprobleem van Fibonacci in de openbaarheid gebracht heeft).

5.2.3 Niet-homogene lineaire recurrente betrekkingen met constante coëfficiënten

Wij zullen de oplossingsmethode bespreken voor enkele eenvoudige gevallen van niet-homogene lineaire betrekkingen met constante coëfficiënten

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + f(n), \quad n \geq k, \tag{5.11}$$

waarbij $f \neq 0$ (dit betekent: er bestaat een $n \geq k$ waarvoor $f(n) \neq 0$). Zoals bij de homogene betrekkingen is de algemene oplossing van dergelijke vergelijking van de orde k afhankelijk van de k vrijheidsgraden $a_0, a_1, \ldots, a_{k-1}$. Elke particuliere oplossing wordt gegeven door specifieke waarden toe te kennen aan deze vrijheidsgraden. Veronderstel dat we een particuliere oplossing $a_n^{(p)}$ kennen die correspondeert met de waarden $a_0^{(p)}, a_1^{(p)}, \ldots, a_{k-1}^{(p)}$ van de vrijheidsgraden, zodat dus

$$a_n^{(p)} = \lambda_1 a_{n-1}^{(p)} + \lambda_2 a_{n-2}^{(p)} + \cdots + \lambda_k a_{n-k}^{(p)} + f(n).$$

Beschouw anderzijds de corresponderende *homogene* lineaire recurrente betrekking

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k},$$

en veronderstel dat we de algemene oplossing $a_n^{(h)}$ van deze homogene betrekking gevonden hebben. Dan volgt uit Stelling 5.2.1 onmiddellijk dat de algemene oplossing van de oorspronkelijke betrekking (5.11) gegeven wordt door

$$a_n = a_n^{(h)} + a_n^{(p)}.$$

De algemene oplossing van een niet-homogene lineaire recurrente betrekking met constante coëfficiënten is bijgevolg de som van een particuliere oplossing van deze vergelijking en de algemene oplossing van de bijhorende homogene lineaire betrekking.

De vraag is nu natuurlijk hoe we die ene particuliere oplossing kunnen vinden. Een algemene oplossingsmethode is moeilijk aan te geven. In de volgende stelling zullen we zien dat in enkele bijzondere gevallen er wel een methode te vinden is. We laten het bewijs achterwege.

Stelling 5.2.3. *Veronderstel dat de volgende lineaire recurrente betrekking met constante coëfficiënten gegeven is*

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + f(n). \tag{5.12}$$

(1) *Indien $f(n)$ een veelterm is van de graad ℓ, dan is een particuliere oplossing van de vorm*

$$a_n^{(p)} = \alpha_0 n^t + \alpha_1 n^{t+1} + \cdots + \alpha_\ell n^{t+\ell}.$$

Hierbij is t $(0 \leq t \leq k)$ de multipliciteit van 1 als oplossing van de karakteristieke vergelijking van de bijhorende homogene recurrente betrekking. De coëfficiënten $\alpha_0, \alpha_1, \ldots, \alpha_\ell$ worden bepaald door substitutie in de vergelijking (5.12).

(2) *Indien $f(n) = cq^n$ met c een constante, dan is*

$$a_n^{(p)} = \alpha n^t q^n$$

een particuliere oplossing. Hierbij is t $(0 \leq t \leq k)$ de multipliciteit van q in de karakteristieke vergelijking van de bijhorende homogene betrekking. De waarde van α kan bepaald worden door substitutie van de particuliere oplossing in de vergelijking (5.12).

Zonder bewijs. □

We zullen deze stelling illustreren aan de hand van enkele voorbeelden.

Voorbeelden

1. *Zoek de algemene oplossing van de recurrente betrekking*

$$a_n = 5a_{n-1} - 6a_{n-2} + 6 \cdot (4)^n, \quad n \geq 2.$$

Oplossing.

De bijhorende homogene recurrente betrekking hebben we reeds vroeger opgelost, $a_n^{(h)} = \alpha_1 2^n + \alpha_2 3^n$ (zie (5.10)). Aangezien 4 geen oplossing

is van de karakteristieke vergelijking, is een particuliere oplossing van de niet-homogene betrekking van de vorm

$$a_n^{(p)} = \alpha \cdot (4)^n.$$

Substitueren we dit in de gegeven vergelijking, dan bekomen wij:

$$\alpha \cdot (4)^n = 5\alpha \cdot (4)^{n-1} - 6\alpha \cdot (4)^{n-2} + 6 \cdot (4)^n, \quad n \geq 2.$$

Hieruit volgt dat

$$\alpha((4)^2 - 5 \cdot (4) + 6) = 6 \cdot (4)^2.$$

Bijgevolg is $\alpha = 48$. De algemene oplossing van de gegeven recurrente betrekking is bijgevolg

$$a_n = \alpha_1 2^n + \alpha_2 3^n + 48 \cdot (4)^n.$$

2. *Bereken de som van de kwadraten van de elementen uit* $\mathbb{N}[0, n]$.

Oplossing.

De recurrente betrekking die hierbij behoort, is $a_n = a_{n-1} + n^2$, met $a_0 = 0$. De bijhorende homogene recurrente betrekking heeft algemene oplossing $a_n^{(h)} = \alpha$. Aangezien echter 1 een enkelvoudige oplossing is van de karakteristieke vergelijking van de homogene betrekking, is een goede keuze voor de particuliere oplossing

$$a_n^{(p)} = \alpha_0 n + \alpha_1 n^2 + \alpha_2 n^3.$$

Bijgevolg is de algemene oplossing van de niet-homogene recurrente betrekking gegeven door:

$$a_n = \alpha + \alpha_0 n + \alpha_1 n^2 + \alpha_2 n^3.$$

Aangezien echter $a_0 = 0$, volgt hieruit dat $\alpha = 0$. Indien we deze oplossing nu substitueren in de betrekking, dan bekomen we

$$\begin{aligned}
&\alpha_0 n + \alpha_1 n^2 + \alpha_2 n^3 \\
&\quad = \alpha_0(n-1) + \alpha_1(n-1)^2 + \alpha_2(n-1)^3 + n^2 \\
&\quad = (-\alpha_0 + \alpha_1 - \alpha_2) + (\alpha_0 - 2\alpha_1 + 3\alpha_2)n + (\alpha_1 - 3\alpha_2 + 1)n^2 + \alpha_2 n^3.
\end{aligned}$$

Bijgevolg zijn $\alpha_0, \alpha_1, \alpha_2$ oplossingen van het stelsel

$$\begin{cases}
\alpha_1 = \alpha_1 - 3\alpha_2 + 1 \\
\alpha_0 = \alpha_0 - 2\alpha_1 + 3\alpha_2 \\
0 = -\alpha_0 + \alpha_1 - \alpha_2.
\end{cases}$$

Hieruit volgt dat $\alpha_0 = 1/6, \alpha_1 = 1/2$ en $\alpha_2 = 1/3$. Bijgevolg is

$$\sum_{k=0}^{n} k^2 = \frac{1}{6}n + \frac{1}{2}n^2 + \frac{1}{3}n^3 = \frac{n(n+1)(2n+1)}{6}.$$

3. *Op een tafel worden 3 staven A, B, C bevestigd. Men beschikt over n ronde platte schijven (van verschillende grootte), telkens met een opening in het midden (zodat ze over de staven geschoven kunnen worden). De schijven die over een zelfde staaf geschoven liggen, moeten steeds mooi geordend liggen van groot (onderaan) tot klein (bovenaan). Stel dat alle schijven gestapeld liggen over staaf A. In hoeveel bewegingen kan men deze toren dan naar de staaf C verhuizen wanneer slechts 1 schijf per keer verplaatst kan worden? De staaf B mag hierbij gebruikt worden als hulpstaaf. Dit probleem wordt soms het probleem van de* torens van Hanoi *genoemd.*

Oplossing.

Om a_n te berekenen, redeneren we als volgt:

(a) We moeten a_{n-1} bewegingen uitvoeren om de $n-1$ bovenste schijven van de staaf A naar de staaf B te brengen. Hierbij dient C als hulpstaaf.

(b) Om de overblijvende schijf op staaf A naar staaf C te brengen hebben we 1 beweging nodig.

(c) De $n-1$ schijven van staaf B worden nu met a_{n-1} bewegingen naar schijf C gebracht waarbij schijf A als hulpstaaf gebruikt wordt.

De recurrente betrekking die bij het probleem behoort, is bijgevolg

$$a_n = 2a_{n-1} + 1, \quad n \geq 1, \quad a_0 = 0. \tag{5.13}$$

De algemene oplossing $a_n^{(h)}$ van de homogene betrekking is $a_n^{(h)} = \alpha_0 2^n$. Aangezien 1 geen oplossing is van de karakteristieke vergelijking, is een particuliere oplossing van (5.13) van de vorm $a_n^{(p)} = \alpha$. Indien we dit in (5.13) substitueren, dan verkrijgen we $\alpha = -1$. Bijgevolg is de algemene oplossing van deze vergelijking gegeven door

$$a_n = \alpha_0 2^n - 1.$$

Aangezien echter $a_0 = 0$ is $\alpha_0 = 1$, zodat we dus $2^n - 1$ bewegingen nodig hebben om de toren volgens de regels van het spel van A naar C te verplaatsen.

Oefeningen

1. Los volgende recurrente betrekkingen op.

   (a) $a_n = 2a_{n-1} + n + 1,\ n \geq 1,\ a_0 = 1.$

   (b) $a_n = 9a_{n-2} + 8n$ met $4a_0 = 9$ en $4a_1 = 1$.

2. Iemand leent geld van een bank en betaalt hiervoor jaarlijks een vast bedrag s aan de bank. Een gedeelte van de jaarlijkse betaling is de rente over de schuld volgens een vast percentage r, de rest van de betaling wordt gebruikt om de schuld te verminderen.

   (a) Als a_{n-1} de schuld is na $n-1$ jaar, wat is dan de schuld na n jaar?

   (b) Geef de algemene oplossing van de recurrente betrekking die bij het probleem behoort.

   (c) Bereken de jaarlijkse betaling s aan de bank, als de persoon een bedrag K leende en zijn schuld in p jaar moet aflossen.

3. Een verzameling rechten noemt men willekeurig gelegen in het vlak als geen twee van die rechten evenwijdig zijn en geen drie ervan door een zelfde punt gaan. Bepaal het aantal gebieden waarin het vlak door n willekeurig gelegen rechten verdeeld wordt.

5.3 Recurrente betrekkingen en voortbrengende functies

We hebben reeds uitvoerig besproken hoe we met een rij $(a_k)_{k\in\mathbb{N}}$ een voortbrengende functie kunnen associëren. Indien de rij nu recursief gedefinieerd wordt, kunnen we ons de vraag stellen hoe we rechtstreeks van de recurrente betrekking kunnen overgaan naar de voortbrengende functie. Het antwoord op deze vraag voor de homogene lineaire recurrente betrekkingen met constante coëfficiënten wordt in de volgende stelling gegeven.

Stelling 5.3.1. *Indien een rij $(a_k)_{k\in\mathbb{N}}$ recursief gedefinieerd wordt door*

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k}, \quad n \geq k,$$

met vrijheidsgraden $a_0, a_1, \ldots, a_{k-1}$, dan wordt de voortbrengende functie $g(x)$ van deze rij gegeven door

$$g(x) = \frac{h(x)}{1 - \lambda_1 x - \cdots - \lambda_k x^k}.$$

Hierbij is $h(x)$ een veelterm met graad kleiner dan k die volledig bepaald wordt door de waarden van de vrijheidsgraden $a_0, a_1, \ldots, a_{k-1}$.

Bewijs. Beschouw het product

$$g(x)(1 - \lambda_1 x - \cdots - \lambda_k x^k) = \Big(\sum_{l=0}^{\infty} a_l x^l\Big)(1 - \lambda_1 x - \cdots - \lambda_k x^k).$$

De coëfficiënt van x^n $(n \geq k)$ in dit product is gelijk aan

$$a_n - \lambda_1 a_{n-1} - \lambda_2 a_{n-2} - \cdots - \lambda_k a_{n-k},$$

en is bijgevolg gelijk aan 0. De enige coëfficiënten in de uitwerking die eventueel verschillend van 0 kunnen zijn, zijn de coëfficiënten van x^l met $0 \leq l \leq k-1$. Bijgevolg is $h(x)$ een veelterm van de graad kleiner dan k. Merk op dat

$$h(x) = a_0 + (a_1 - \lambda_1 a_0)x + \cdots + (a_{k-1} - \lambda_1 a_{k-2} - \cdots - \lambda_{k-1} a_0)x^{k-1}.$$

Deze veelterm is dus inderdaad volledig bepaald door de waarden van de vrijheidsgraden. □

Opmerking

Merk op dat de noemer $1 - \lambda_1 x - \cdots - \lambda_k x^k$ van de voortbrengende functie $g(x)$, veel gelijkenis vertoont met de karakteristieke vergelijking $x^k - \lambda_1 x^{k-1} - \cdots - \lambda_k = 0$ die bij de homogene recurrente betrekking behoort.

Voorbeeld

Bepaal de voortbrengende functie van de rij $(a_n)_{n\in\mathbb{N}}$ die recursief gedefinieerd wordt door $a_0 = 1$, $a_1 = 5$ en $a_n = 5a_{n-1} - 6a_{n-2}$ voor $n \geq 2$.

Oplossing.
We hebben deze rij reeds eerder ontmoet en we hebben bewezen dat $a_n = 3^{n+1} - 2^{n+1}$. De voortbrengende functie is wegens bovenstaande stelling van de vorm

$$g(x) = \frac{h(x)}{1 - 5x + 6x^2}.$$

Hierbij is $h(x) = a_0 + (a_1 - 5a_0)x = 1$. Bijgevolg is

$$g(x) = \frac{1}{1 - 5x + 6x^2}.$$

Merk op dat we $g(x)$ kunnen schrijven als (zie splitsen in partieelbreuken, cursus analyse)

$$\begin{aligned} g(x) &= \frac{3}{1-3x} - \frac{2}{1-2x} \\ &= 3\sum_{k=0}^{\infty}(3x)^k - 2\sum_{k=0}^{\infty}(2x)^k. \end{aligned}$$

Hetgeen nog maar eens bevestigt dat $a_n = 3^{n+1} - 2^{n+1}$.

5.4 Zuinig en onzuinig sorteren

Veronderstel dat we n items op de één of andere manier willen sorteren. Het kunnen getallen zijn die op grootte gesorteerd worden, of namen die op alfabet gerangschikt moeten worden. Een voor de hand liggende manier is te beginnen met één enkel item, en dan de items één voor één op de juiste plaats invoegen. Dergelijke methode wordt soms *bubble-sort* genoemd. Deze methode kan echter zeer veel rekentijd in beslag nemen. Inderdaad, indien de rij reeds $n-1$ items bevat, dan zullen in het slechtste geval $n-1$ stappen nodig zijn om het volgende item op de juiste plaats te zetten. Indien men een rij getallen aangeboden krijgt die van klein naar groot gesorteerd is, en men moet ze sorteren van groot naar klein, dan zal dus de meest ongunstige situatie optreden. Het aantal stappen a_n die we in dit geval nodig hebben voldoet dan aan de recurrente betrekking $a_n = a_{n-1} + (n-1)$. Hieruit volgt (werk zelf uit) dat $a_n = n(n-1)/2$. Indien n groot is, dan kunnen we stellen dat er in het slechtste geval ruwweg $n^2/2$ stappen nodig zijn om een rij door middel van het bubble-sort algoritme te ordenen. Zelfs indien de rij niet in de meest ongunstige situatie aangeboden wordt, dan zullen er toch gemiddeld ongeveer de helft van het aantal ongunstige stappen nodig zijn. Zodat er in het totaal ongeveer $n^2/4$ stappen ondernomen zullen moeten worden. Men zegt daarom dat het bubble-sort algoritme een complexiteit van de orde n^2 heeft.

Een ander algoritme is het *merge-sort* algoritme. Dit algoritme gebruikt het zogenaamde principe van verdeel en heers. Men splitst de rij in twee gelijke (of ongeveer gelijke) delen. Men sorteert elk van beide delen en men voegt daarna beide gesorteerde delen samen tot een geordend geheel. Dat laatste kost precies zoveel[1] stappen als er items in dat geheel zijn: men

[1] In feite 1 stap minder (om n objecten te vergelijken zijn slechts $n-1$ vergelijkingen nodig), maar we negeren deze ene stap. Om de orde van de complexiteit te bepalen maakt dat overigens geen verschil.

neemt immers telkens de kleinste van beide helften, die twee worden onderling vergeleken en de kleinste van de twee wordt naar de totale rij verplaatst. Hoe sorteert men nu beide helften? Dat gaat precies op dezelfde manier: men deelt ze in twee, beide helften worden gesorteerd en daarna samengevoegd. Als de lengte van zo'n helft gelijk is aan 1, dan hoeft men niets meer te doen. Indien we het aantal stappen die deze methode voor een rij van lengte n gebruikt, aangeven met a_n, dan geldt

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

Merk op dat in deze methode er zich geen gunstige of ongunstige gevallen voordoen. Voor gegeven n duurt het altijd even lang. Veronderstel nu dat $n = 2^k$ en stel $s_k := a_{2^k}$, dan geldt er

$$s_{k+1} = 2s_k + 2^{k+1}, \quad s_0 = 0.$$

Bijgevolg is $s_k = k2^k$ (werk zelf uit). Het totaal aantal stappen door middel van het merge-sort algoritme is bijgevolg voor een rij van lengte $n = 2^k$ ongeveer gelijk aan $n \cdot \log_2 n$. Dit algoritme wordt daarom soms een algoritme met een complexiteit van de orde $n \log n$ genoemd. Men kan bewijzen dat men niet veel zuiniger kan sorteren. Er bestaan wel nog andere sorteeralgoritmen die van dezelfde complexiteitsorde zijn. Indien $n = 1024 = 2^{10}$ zijn er bij het gebruik van het bubble-sort algoritme ongeveer een half miljoen stappen nodig, terwijl bij het gebruik van het merge-sort algoritme ongeveer 10240 stappen nodig zullen zijn.

5.5 Differentierijen

Definitie

Indien een rij $(a_n)_{n\in\mathbb{N}}$ van (reële) getallen gegeven is, dan noteren we $a_n - a_{n-1}$ door $\mathrm{d}(a_n)$. De rij $(\mathrm{d}(a_n))_{n\in\mathbb{N}^*}$ wordt de *differentierij van eerste orde* behorend bij de rij $(a_n)_{n\in\mathbb{N}}$ genoemd. De *differentierij van tweede orde* behorend bij de rij $(a_n)_{n\in\mathbb{N}}$ is per definitie gelijk aan

$$\begin{aligned} (\mathrm{d}^2(a_n))_{n\in\mathbb{N}\setminus\{0,1\}} &:= (\mathrm{d}(\mathrm{d}(a_n)))_{n\in\mathbb{N}\setminus\{0,1\}} \\ &= (\mathrm{d}(a_n) - \mathrm{d}(a_{n-1}))_{n\in\mathbb{N}\setminus\{0,1\}} \\ &= (a_n - 2a_{n-1} + a_{n-2})_{n\in\mathbb{N}\setminus\{0,1\}}. \end{aligned}$$

Algemeen wordt de *differentierij van de k-de orde* behorend bij de rij $(a_n)_{n\in\mathbb{N}}$ gedefinieerd als

$$(\mathrm{d}^k(a_n))_{n\in\mathbb{N}\setminus\{0,1,\ldots,k-1\}} := \left(\mathrm{d}^{k-1}(a_n) - \mathrm{d}^{k-1}(a_{n-1})\right)_{n\in\mathbb{N}\setminus\{0,1,\ldots,k-1\}}.$$

Een *differentievergelijking* is een vergelijking tussen de elementen van een rij $(a_n)_{n\in\mathbb{N}}$ en de elementen van de differentierijen die hierbij behoren. Zo is bijvoorbeeld de vergelijking $3\mathrm{d}^2(a_n) + 2\mathrm{d}(a_n) + 7a_n = 0$ een differentievergelijking waarbij elementen uit de rij $(a_n)_{n\in\mathbb{N}}$ en de differentierijen van eerste en tweede orde betrokken zijn. Daarom wordt deze vergelijking een *homogene differentievergelijking van de tweede orde* genoemd.

Merk op dat

$$a_{n-1} = a_n - \mathrm{d}(a_n), \quad n \geq 1$$

en dat

$$\begin{aligned} a_{n-2} &= a_{n-1} - \mathrm{d}(a_{n-1}) \\ &= (a_n - \mathrm{d}(a_n)) - \mathrm{d}(a_n - \mathrm{d}(a_n)) \\ &= a_n - 2\mathrm{d}(a_n) + \mathrm{d}^2(a_n), \quad n \geq 2. \end{aligned}$$

Bijgevolg kan elke recurrente betrekking als differentievergelijking geschreven worden. Aan de andere kant, kan als gevolg van de definitie van de differentierijen, elke differentievergelijking geschreven worden als een recurrente betrekking. Zo zal bijvoorbeeld de differentievergelijking $3\mathrm{d}^2(a_n)+2\mathrm{d}(a_n)+7a_n = 0$, gelijkwaardig zijn met de recurrente betrekking $12a_n = 8a_{n-1} - 3a_{n-2}$. De methode voor het oplossen van lineaire recurrente betrekkingen van de orde k met constante coëfficiënten kan bijgevolg gebruikt worden om lineaire differentievergelijkingen van de orde k met constante coëfficiënten op te lossen. Om die reden worden de begrippen *differentievergelijkingen* en *recurrente betrekkingen* wel eens door mekaar gebruikt.

Opmerking

In de analyse zou men het verschil $\mathrm{d}(a_n) = a_n - a_{n-1}$ als een eerste benadering van de *differentiaal van de functie* a_n beschouwen en zou men differentievergelijkingen als een benadering van *differentiaalvergelijkingen* beschouwen. De methodes voor het oplossen van lineaire differentievergelijkingen enerzijds en voor het oplossen van lineaire differentiaalvergelijkingen anderzijds zijn daarom ook volledig dezelfde. Het benaderd oplossen van een differentiaalvergelijking via technieken uit de numerieke analyse komt in feite neer op het oplossen van differentievergelijkingen.

Hoofdstuk

6 Getaltheorie

6.1 Basisbegrippen

6.1.1 Deelbaarheid

We beschouwen de volgende relatie $\mathcal{D} \subseteq (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z}$ gedefinieerd door

$$(a, b) \in \mathcal{D} \iff \exists q \in \mathbb{Z} \colon b = a \cdot q.$$

We noemen $\mathcal{D}$ de *deelbaarheidsrelatie* en we zeggen dat a *een deler is van* b of dat b *een* a*-voud* is, of b *is deelbaar door* a of nog dat a *een factor is van* b. Indien $(a, b) \in \mathcal{D}$, dan noteren we dit kort als $a \mid b$, terwijl $a \nmid b$ een verkorte notatie is voor $(a, b) \notin \mathcal{D}$.

Elk geheel getal $b \neq 0$ is uiteraard deelbaar door $1, -1, b$ en $-b$. We noemen deze soms de *onechte delers* van het getal. Al de andere delers worden de *echte delers* van het getal genoemd. Merk op dat dus 1 een deler is van elk geheel getal, en dat elk geheel getal verschillend van 0 een deler is van 0.

Veronderstel $a \mid b$ en $a \mid c$. Dan zal voor alle gehele getallen x en y gelden dat $a \mid (bx + cy)$, in het bijzonder is a dan een deler van $b + c$ en van $b - c$.

In plaats van $2 \mid b$ zeggen we meestal dat b even is, terwijl $2 \nmid b$ betekent dat b oneven is.

Stelling 6.1.1. *Voor elke 2 getallen $a \in \mathbb{N}^*$ en $b \in \mathbb{Z}$ bestaan er unieke gehele getallen q (quotiënt) en r (rest) zodanig dat*

$$b = a \cdot q + r \quad r \in \mathbb{N}[0, a - 1].$$

Bewijs. (a) We tonen eerst aan dat er dergelijke getallen q en r bestaan. We passen het axioma van de goede ordening toe op de volgende verzameling R:

$$R = \{x \in \mathbb{N} \mid b = a \cdot y + x \text{ voor een } y \in \mathbb{Z}\}.$$

We bewijzen eerst dat R niet ledig is. Als $b \geq 0$, dan volgt uit $b = a \cdot 0 + b$ dat $b \in R$. Als $b < 0$, dan geldt $b = a \cdot b + (1 - a) \cdot b$.

Aangezien $(1-a)\cdot b \geq 0$ zal $(1-a)\cdot b \in R$. De verzameling R is dus niet ledig en bezit bijgevolg een kleinste element r. We hebben $b = a\cdot q + r$ voor een zekere $q \in \mathbb{Z}$. Als $r \geq a$, dan hebben we eveneens dat $b = a\cdot(q+1) + (r-a)$ met $r > r-a \geq 0$, in tegenstrijd met de definitie van r. Bijgevolg geldt $r \in \mathbb{N}[0, a-1]$.

(b) We tonen de uniciteit van q en r aan. Onderstel dat $b = a\cdot q_1 + r_1 = a\cdot q_2 + r_2$ voor zekere $q_1, q_2 \in \mathbb{Z}$ en zekere $r_1, r_2 \in \mathbb{N}[0, a-1]$. Als $q_1 > q_2$, dan geldt $r_2 = a\cdot(q_1 - q_2) + r_1 \geq a + r_1 \geq a$, een tegenstrijdigheid. Bijgevolg geldt $q_2 \geq q_1$. We kunnen nu de rol van q_1 en q_2 omkeren, waaruit dan volgt dat $q_1 \geq q_2$, zodat we mogen besluiten dat $q_1 = q_2$ en $r_1 = r_2$. □

Opmerking

Een belangrijk gevolg van deze stelling is, dat voor elk gegeven natuurlijk getal $t \geq 2$, een willekeurig positief geheel getal geschreven kan worden als een lineaire combinatie van machten van t waarbij de coëfficiënten tot de verzameling $\mathbb{N}[0, t-1]$ behoren. Indien we immers de voorgaande stelling herhaalde malen toepassen, dan verkrijgen we:

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ &\vdots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n\,. \end{aligned}$$

Hierbij zal elke rest r_i tot $\mathbb{N}[0, t-1]$ behoren en zal de deling stoppen van zodra $q_n = 0$. Indien we nu de quotiënten q_i elimineren, dan verkrijgen we

$$x = r_n t^n + r_{n-1}t^{n-1} + \cdots + r_1 t + r_0.$$

We schrijven verkort $x = (r_n r_{n-1} \ldots r_0)_t$ en we noemen dit de *ontwikkeling van x in basis t*. De meest gebruikte basissen zijn $t = 10$ (tiendelig getallenstelsel, $r_i \in \mathbb{N}[0,9]$), $t = 2$ (binair getallenstelsel, $r_i \in \mathbb{N}[0,1]$), $t = 8$ (octaal getallenstelsel, $r_i \in \mathbb{N}[0,7]$), en $t = 16$ (hexadecimaal getallenstelsel, $r_i \in \mathbb{N}[0,15]$). Om verwarring te vermijden worden in het hexadecimaal getallenstelsel de getallen 10 tot en met 15 respectievelijk voorgesteld door A, B, C, D, E, en F. We hebben bijvoorbeeld

$$\begin{aligned} (2010)_{10} &= (11111011010)_2 \\ &= (3732)_8 \\ &= (7DA)_{16}\,. \end{aligned}$$

6.1.2 Priemgetallen

Een positief geheel getal p wordt een *priemgetal* genoemd als p juist 2 positieve delers bezit (1 en zichzelf). In het bijzonder is 1 geen priemgetal. Elk getal $m \in \mathbb{N} \setminus \{0, 1\}$ dat geen priemgetal is, kan dus geschreven worden als een product $m_1 m_2$ met $m_i \in \mathbb{N}[2, m-1]$ (m_1 kan gelijk zijn aan m_2). We noemen daarom elk dergelijk getal m een *samengesteld getal* .

De lijst van de priemgetallen kleiner dan 50 is eenvoudig op te schrijven:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Nochtans is het voor grotere getallen niet altijd zo eenvoudig om snel te bepalen of een getal een priemgetal is. Het probleem om al de priemgetallen kleiner dan een gegeven positief geheel getal op te sommen is een ander probleem. Wij zullen in dit hoofdstuk enkele technieken bespreken om deze twee problemen aan te pakken.

Merk vooreerst op dat er oneindig veel priemgetallen bestaan. Dit is een stelling die toegeschreven is aan Euclides.

Stelling 6.1.2 (Euclides)**.** *De verzameling van de priemgetallen is een oneindige verzameling.*

Bewijs. Veronderstel dat de verzameling van de priemgetallen een eindige verzameling $\{p_1, p_2, \ldots, p_n\}$ zou zijn. Stel $m = \prod_{i=1}^{n} p_i$, dan is $m + 1$ dus geen priemgetal en dus bezit $m + 1$ eigenlijke delers. Noem q de kleinste eigenlijke positieve deler van $m + 1$. Dan is q een priemgetal en dus ook een deler van m. Bijgevolg is q een deler van $(m + 1) - m = 1$. Dit is een tegenstrijdigheid. Bijgevolg is de verzameling van de priemgetallen een oneindige verzameling. □

6.1.3 Ontbinden in priemfactoren

Wij zijn vertrouwd met de idee dat elk natuurlijk getal (verschillend van 0 en 1) geschreven kan worden als een product van priemfactoren, of m.a.w. ontbonden kan worden in priemfactoren. Deze eigenschap is echter een gevolg van het axioma van de goede ordening.

Stelling 6.1.3. *Elk getal $n \in \mathbb{N} \setminus \{0, 1\}$ is te schrijven als een product van priemfactoren.*

Bewijs. We passen het principe van het kleinste tegenvoorbeeld toe (zie p. 19). Veronderstel dus dat $m \in \mathbb{N} \setminus \{0, 1\}$ een kleinste tegenvoorbeeld is op de stelling, m.a.w. het kleinste getal in $\mathbb{N} \setminus \{0, 1\}$ dat niet te schrijven is

als product van priemfactoren. Dan kan m in het bijzonder zelf geen priemgetal zijn, en dus moet m samengesteld zijn: stel $m = m_1 m_2,\ m_i \in \mathbb{N}[2, m-1]$. Aangezien echter m het *kleinste* tegenvoorbeeld was, bezitten zowel m_1 als m_2 een ontbinding in priemfactoren. Het product $m = m_1 m_2$ bezit dan echter eveneens een ontbinding in priemfactoren, en dit is tegen de onderstelling dat m een *tegenvoorbeeld* was. Deze contradictie besluit het bewijs. □

We zullen verder (zie Stelling 6.2.4) zien dat elk getal $n \in \mathbb{N} \setminus \{0, 1\}$ op *unieke manier* te schrijven is als een product van priemfactoren.

De zeef van Eratosthenes

De vlugste manier om alle priemgetallen te vinden die kleiner zijn dan een gegeven getal n staat bekend als de *Zeef van Eratosthenes*. Deze methode gaat als volgt. Het getal 2 is een priemgetal, en al de andere even getallen zijn uiteraard geen priemgetallen. We kunnen ons dus beperken tot de oneven getallen, kleiner dan n. We rangschikken deze getallen van klein naar groot. Het eerste getal in de rij is 3, een priemgetal, maar alle 3-vouden mogen we schrappen. Het volgende getal is het priemgetal 5, de 5-vouden worden geschrapt, daarna komt 7 en worden al de 7-vouden geschrapt. Merk op dat 9 reeds geschrapt was als 3-voud, zodat het volgende priemgetal 11 zal zijn, ... Telkens we een getal tegenkomen dat nog niet geschrapt is, weten we dat het geen eigenlijke delers bezit en dus een priemgetal is. We schrappen telkens de veelvouden van dit getal (sommige van deze getallen kunnen al eerder geschrapt zijn). We kunnen ophouden van zodra we aan een priemgetal komen dat groter is dan $\sqrt{n}$ (waarom?). Merk op dat deze methode zeker niet geschikt is als efficiënte priemtest! (Het vinden van efficiënte algoritmen om te controleren of een gegeven getal priem is, steunt vaak op zeer diepgaande wiskundige resultaten, en maakt deel uit van het vakgebied dat men *computeralgebra* noemt.)

6.2 Grootste gemene deler en kleinste gemeen veelvoud

Voor elke twee gehele getallen a, b noemen we een geheel getal d dat zowel a als b deelt, een *gemene deler* van a en b. Als a en b niet beide nul zijn, dan hebben a en b slechts eindig veel delers gemeen, en dus is er dan een grootste gemene deler van a en b, die we noteren door $\gcd(a, b)$. Merk op dat de grootste gemene deler steeds een natuurlijk getal is. Veronderstel dat a en b positieve natuurlijke getallen zijn, dan wordt elk getal dat een positief

veelvoud is van zowel a als b een *gemeen veelvoud* van a en b genoemd. Het kleinste onder de positieve gemene veelvouden noemen we het *kleinste gemeen veelvoud* van a en b, en we noteren dit door $\text{lcm}(a, b)$.

Getallen a en b met $\gcd(a, b) = 1$ noemen we *onderling ondeelbaar*. We kunnen ook zeggen dat $\gcd(a, b) = 1$ betekent dat a en b geen priemfactoren gemeen hebben. Daarom worden in dit geval ook a en b *relatief priem* of *copriem* genoemd.

Er is een zeer efficiënt algoritme om de grootste gemene deler van twee gehele getallen te berekenen, het zogenaamde *algoritme van Euclides*.

Dit algoritme steunt op het feit dat elke deler van a en b eveneens een deler is van $a \pm b$ zodat, in de veronderstelling dat $b = aq + r$ moet gelden dat $\gcd(a, b) = \gcd(a, r)$.

Bijgevolg kunnen we, om de grootste gemene deler van twee positieve natuurlijke getallen a en b te berekenen, als volgt te werk gaan. We definieren q_i en r_i recursief door middel van de volgende vergelijkingen:

$$\begin{aligned} b &= aq_1 + r_2 && r_2 \in \mathbb{N}[0, b-1] \\ a &= r_2q_2 + r_3 && r_3 \in \mathbb{N}[0, r_2 - 1] \\ r_2 &= r_3q_3 + r_4 && r_4 \in \mathbb{N}[0, r_3 - 1] \\ &\vdots \end{aligned}$$

Aangezien elke rest r_i steeds strikt kleiner is dan de vorige, zal dit proces zeker stoppen na een eindig aantal stappen, namelijk als de rest r_{k+1} nul wordt. De laatste stappen zien er dan als volgt uit:

$$\begin{aligned} r_{k-3} &= r_{k-2}q_{k-2} + r_{k-1} && r_{k-1} \in \mathbb{N}[0, r_{k-2} - 1] \\ r_{k-2} &= r_{k-1}q_{k-1} + r_k && r_k \in \mathbb{N}[0, r_{k-1} - 1] \\ r_{k-1} &= r_kq_k. && (r_{k+1} = 0) \end{aligned}$$

De gevraagde grootste gemene deler is dan r_k. Dit algoritme is niet alleen in de praktijk zeer belangrijk, maar bezit ook heel wat theoretische gevolgen, zoals de volgende stelling aantoont.

Stelling 6.2.1 (Stelling van Bézout)**.** *Veronderstel dat a en b gehele getallen zijn (niet beide nul), en dat $d = \gcd(a, b)$, dan bestaan er gehele getallen m en n zodanig dat $am + bn = d$.*

Bewijs. We gebruiken de notatie die we hierboven ingevoerd hebben bij het uiteenzetten van het algoritme van Euclides, en we stellen bovendien $r_1 = a$ en $r_0 = b$; we zullen aantonen dat d een lineaire combinatie is van $r_{\ell-1}$ en r_ℓ

voor elke $\ell \in \{1, \ldots, k-1\}$, van achter naar voor (dus eerst voor $\ell = k-1$, vervolgens voor $\ell = k-2$, enzovoort, tot we uiteindelijk aan $\ell = 1$ aankomen.)

Omdat $d = r_k$, kunnen we de voorlaatste vergelijking herschrijven als

$$d = r_{k-2} - q_{k-1} r_{k-1},$$

en dus is d een lineaire combinatie van r_{k-2} en r_{k-1}.

Veronderstel nu dat we reeds weten dat $d = \lambda r_{\ell-1} + \mu r_\ell$ voor zekere $\lambda, \mu \in \mathbb{Z}$; we tonen dan aan dat d ook een lineaire combinatie is van $r_{\ell-2}$ en $r_{\ell-1}$. Inderdaad, uit de vergelijking

$$r_{\ell-2} = r_{\ell-1} q_{\ell-1} + r_\ell$$

volgt dat

$$\begin{aligned} d &= \lambda r_{\ell-1} + \mu(r_{\ell-2} - r_{\ell-1} q_{\ell-1}) \\ &= \mu r_{\ell-2} + (\lambda - \mu q_{\ell-1}) \cdot r_{\ell-1}, \end{aligned}$$

zodat d ook een lineaire combinatie is van $r_{\ell-2}$ en $r_{\ell-1}$. Door dit argument herhaaldelijk toe te passen, vinden we uiteindelijk dat d een lineaire combinatie is van r_0 en r_1, wat we wilden bewijzen. □

Gevolgen

Deze stelling wordt vaak toegepast in het geval a en b onderling priem zijn, aangezien er dan gehele getallen m en n gevonden kunnen worden zodat $ma + nb = 1$. Merk wel op dat de getallen m en n niet noodzakelijk uniek bepaald zijn.

Bovendien kunnen heel wat eigenschappen van de grootste gemene deler en het kleinste gemeen veelvoud als gevolg van deze stelling bewezen worden. Wij vatten deze eigenschappen in de volgende stelling samen, en we laten het bewijs als oefening.

Stelling 6.2.2. (1) *Als voor drie gehele getallen a, b en c geldt dat $c \mid ab$ en dat $\gcd(b, c) = 1$, dan is $c \mid a$.*

(2) *Als a, b en c natuurlijke getallen zijn, en ab en ac niet beide nul zijn, dan is $\gcd(ab, ac) = a \gcd(b, c)$.*

(3) *Als a, b, c getallen zijn (a en b niet beide nul), zodanig dat c deelbaar is door a en b, dan is c deelbaar door $\dfrac{ab}{\gcd(a, b)}$.*

(4) *Als a en b natuurlijke getallen zijn, niet beide nul, dan is $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = ab$.*

(5) *Als a, b en c getallen zijn met hetzij a en b, hetzij a en c, hetzij b en c relatief priem, dan geldt* $\gcd(a,c) \cdot \gcd(b,c) = \gcd(ab,c)$. *Bijgevolg zijn ab en c relatief priem dan en slechts dan als zowel a en c als b en c relatief priem zijn.*

Een andere eigenschap die ons vertrouwd voorkomt, is dat elke ontbinding in priemfactoren van een gegeven natuurlijk getal uniek is, op de volgorde na. Deze eigenschap is terug een gevolg van het axioma van de goede ordening. We bewijzen eerst een andere stelling.

Stelling 6.2.3. *Indien p een priemgetal is en indien $x_1, x_2, \ldots, x_n$ gehele getallen zijn zodanig dat*

$$p \Big| \prod_{i=1}^{n} x_i,$$

dan is p een deler van ten minste één x_i ($i \in \mathbb{N}[1,n]$).

Bewijs. Het volstaat om te bewijzen dat indien $p \mid ab$ met $a, b \in \mathbb{Z}$, dan $p \mid a$ of $p \mid b$. Het algemene resultaat volgt dan per inductie op n.

Stel dus dat $p \mid ab$, en veronderstel dat $p \nmid a$ en $p \nmid b$; dan is $\gcd(a,p) = \gcd(b,p) = 1$. We passen nu Stelling 6.2.2(5) toe met $c = p$, en we zien dat

$$1 \cdot 1 = \gcd(a,p) \cdot \gcd(b,p) = \gcd(ab,p) = p,$$

een contradictie. We besluiten dat het onmogelijk is dat $p \nmid a$ en $p \nmid b$, en dus deelt p ten minste één van de getallen a en b. □

Stelling 6.2.4. *De ontbinding van een natuurlijk getal $n \geq 2$ in priemfactoren is uniek op de orde van de factoren na.*

Bewijs. Als gevolg van het axioma van de goede ordening, mogen we veronderstellen dat indien de bewering niet waar is, dat er dan een kleinste natuurlijk getal $n_0 \geq 2$ bestaat waarvoor dit niet waar is. Veronderstel daarom dat

$$n_0 = \prod_{i=1}^{k} p_i = \prod_{j=1}^{l} p'_j,$$

waarbij p_i ($i \in \mathbb{N}[1,k]$), evenals p'_j ($j \in \mathbb{N}[1,l]$) (niet noodzakelijk onderling verschillende) priemgetallen zijn. Hieruit volgt dat $p_1 \mid \prod_{j=1}^{l} p'_j$, en dus wegens voorgaande stelling dat p_1 ten minste één van de getallen p'_j deelt. Zonder de algemeenheid te schaden, mogen we veronderstellen dat $p_1 \mid p'_1$.

Aangezien beide getallen echter priemgetallen zijn, volgt hieruit dat $p_1 = p'_1$, zodat

$$\frac{n_0}{p_1} = n_1 = \prod_{i=2}^{k} p_i = \prod_{j=2}^{l} p'_j.$$

Dit is echter in strijd met de veronderstelling dat n_0 het kleinste getal is dat twee verschillende ontbindingen in priemfactoren bezit. Bijgevolg bestaat n_0 niet en mogen we besluiten dat de stelling bewezen is voor elke $n \geq 2$. $\square$

Gevolgen

1. Het aantal positieve delers van een natuurlijk getal n kan op de volgende manier berekend worden. Veronderstel dat de ontbinding van n in priemfactoren er als volgt uitziet:

   $$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}.$$

   Elke deler d van n is dan van de vorm

   $$d = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}, \quad x_i \in \mathbb{N}[0, e_i], i = 1, \dots, k.$$

   Het aantal delers van n is bijgevolg gelijk aan het aantal k-tallen $(x_1, x_2, \dots, x_k)$ met $x_i \in \mathbb{N}[0, e_i]$ en is bijgevolg gelijk aan $\prod_{i=1}^{k}(e_i + 1)$.

2. De grootste gemene deler van twee natuurlijke getallen a en b verschillend van 0, heeft een ontbinding in priemfactoren van de vorm $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, waarbij elk van de priemgetallen p_i een gemene deler is van a en van b, en waarbij e_i het minimum is van de exponent van p_i in de priemfactorontbindingen van a en b.

3. Het kleinste gemeen veelvoud van 2 natuurlijke getallen a en b verschillend van 0, heeft een ontbinding in priemfactoren van de vorm $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, waarbij elk van de priemgetallen p_i ten minste één maal voorkomt in de priemfactorontbinding van a of van b, en waarbij e_i het maximum is van de exponent van p_i in deze priemfactorontbindingen van a en b.

Oefeningen

1. Bewijs dat $4^{2n} - 1$ $(n \geq 1)$ steeds deelbaar is door 15.

2. Zoek de grootste gemene deler d van 1320 en 714 en zoek gehele getallen x en y zodanig dat $d = 1320x + 714y$.

3. Zoek een koppel $(x, y) \in \mathbb{Z}^2$ waarvoor geldt dat $325x + 26y = 91$.

4. Zij $a, b \in \mathbb{N}^*$ met $\gcd(a, b) = 1$. Toon aan dat $\gcd(a + b, a - b)$ gelijk is aan 1 of 2.

5. Bewijs dat $\sqrt{2}$ een irrationaal getal is.

6. Bewijs dat er geen gehele getallen $x,\ y,\ z,\ u$ bestaan waarvoor $x^2 + y^2 - 3z^2 - 3u^2 = 0$.

Stelling 6.2.5. *Zij n een positief natuurlijk getal, en $a_0, \ldots, a_n$ gehele getallen, met $a_0 \neq 0$ en $a_n \neq 0$. Dan geldt voor elke rationale oplossing x_0 van de vergelijking*

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

dat $x_0 = p/q$, voor een zekere p die deler is van a_n, en voor een zekere q die deler is van a_0. In het bijzonder, als $a_0 = 1$, dan zijn de rationale oplossingen ook geheel.

Bewijs. Laten we een rationale oplossing x_0 schrijven als een onvereenvoudigbare breuk, dus $x_0 = p/q,\ \gcd(p, q) = 1$. Dan geldt

$$a_0 (p/q)^n + a_1 (p/q)^{n-1} + \cdots + a_{n-1}(p/q) + a_n = 0.$$

Vermenigvuldiging met q^n levert

$$a_0 p^n + a_1 p^{n-1} q + \cdots + a_{n-1} p q^{n-1} + a_n q^n = 0.$$

Hieruit volgt dat

$$p(a_0 p^{n-1} + a_1 p^{n-2} q + \cdots + a_{n-1} q^{n-1}) = -a_n q^n,$$

zodat p een deler is van $a_n q^n$. Aangezien echter p en q relatief priem zijn, moet p een deler zijn van a_n. Op dezelfde manier bewijzen we dat q een deler is van a_0. □

6.3 De Euler functie

Veronderstel dat n een positief natuurlijk getal is, dan noteren we met $\Phi(n)$ het aantal natuurlijke getallen uit $\mathbb{N}[1, n]$ die copriem zijn met n. De functie Φ wordt de *Euler functie* of *indicator van Euler* genoemd naar Leonhard Euler (1707–1783). Indien $n = p$ een priemgetal is, dan is duidelijk

$$\Phi(p) = p - 1.$$

In de volgende stelling geven we een expliciete formule voor $\Phi(n)$ in het algemeen geval.

Stelling 6.3.1. *Veronderstel dat $n \geq 2$ een natuurlijk getal is met priemfactorontbinding $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Dan is*

$$\Phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right). \tag{6.1}$$

Bewijs. Noem A_j de deelverzameling van $\mathbb{N}[1, n]$ die de veelvouden van p_j bevat $(1 \leq j \leq k)$. Dan geldt

$$\begin{aligned}\Phi(n) &= n - |A_1 \cup A_2 \cup \cdots \cup A_k| \\ &= n - \alpha_1 + \alpha_2 - \cdots + (-1)^k \alpha_k.\end{aligned}$$

Hierbij is (zie stelling 2.10.3) α_i de som van de kardinaalgetallen van al de mogelijke doorsneden die men kan vormen met i dergelijke verzamelingen. De doorsnede van i dergelijke verzamelingen, zoals

$$A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_i}$$

bevat de veelvouden in $\mathbb{N}[1, n]$ van $P = p_{j_1} p_{j_2} \dots p_{j_i}$, en bevat bijgevolg de natuurlijke getallen

$$P, 2P, \dots, \left(\frac{n}{P}\right) P.$$

Deze doorsnede bevat bijgevolg n/P getallen, en α_i is de som van alle termen van de vorm

$$\frac{n}{P} = n\left(\frac{1}{p_{j_1}}\right)\left(\frac{1}{p_{j_2}}\right)\cdots\left(\frac{1}{p_{j_i}}\right).$$

Hieruit volgt nu dat

$$\begin{aligned}\Phi(n) = n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k}\right) + n\left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots + \frac{1}{p_{k-1} p_k}\right) \\ - \cdots + (-1)^k n\left(\frac{1}{p_1 p_2 \cdots p_k}\right) \qquad (6.2) \\ = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right). \qquad \square\end{aligned}$$

Opmerking

We kunnen de formule voor de functie $\Phi(n)$ met $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ ook in de volgende vorm schrijven:

$$\Phi(n) = p_1^{e_1 - 1}(p_1 - 1) p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1)$$

$$= \prod_{i=1}^{k} \left(p_i^{e_i - 1}(p_i - 1) \right). \tag{6.3}$$

Van zodra we de priemfactorontbinding van n hebben opgesteld kunnen we vrij vlug $\Phi(n)$ bepalen. Zo is bijvoorbeeld

$$\Phi(120) = \Phi(2^3 \cdot 3 \cdot 5) = 2^2 \cdot 2 \cdot 4 = 32$$

en

$$\Phi(1680) = \Phi(2^4 \cdot 3 \cdot 5 \cdot 7) = 2^3 \cdot 2 \cdot 4 \cdot 6 = 384.$$

Anderzijds volgt uit de formule (6.2) dat er een term $\frac{n}{d}$ optreedt voor elke deler d van n bestaande uit een product van verschillende priemgetallen, en dit met een coëfficiënt $+1$ of -1 naargelang dit aantal priemgetallen in d even of oneven is. Deze eigenschap kan enigszins veralgemeend worden, zoals we verder zullen uiteenzetten.

We bewijzen eerst echter nog 2 belangrijke eigenschappen van deze Euler functie.

Stelling 6.3.2. (1) *Indien m en n geen gemeenschappelijke priemfactoren bezitten, dan is $\Phi(mn) = \Phi(m) \cdot \Phi(n)$.*

(2) *Voor elk natuurlijk getal n geldt dat $\sum_{d|n} \Phi(d) = n$, waarbij gesommeerd wordt over al de mogelijke delers van het getal n.*

Bewijs. (1) Dit volgt onmiddellijk uit de formule (6.3) voor de Euler functie.

(2) Het aantal positieve breuken kleiner dan of gelijk aan 1 en met noemer gelijk aan n, m.a.w. van de vorm

$$\frac{k}{n} \qquad \text{met } k \leq n$$

is uiteraard gelijk aan n. Als we deze breuken nu zo ver mogelijk vereenvoudigen, dan krijgen we voor elke deler d van n een aantal breuken van de vorm

$$\frac{j}{d} \qquad \text{met } j \leq d \qquad \text{en } \gcd(j, d) = 1.$$

Voor elke d zijn er bijgevolg $\Phi(d)$ dergelijke breuken. Elk van de n breuken heeft juist één vereenvoudigde vorm, zodat

$$\sum_{d|n} \Phi(d) = n. \qquad \square$$

6.4 De Möbius functie

6.4.1 Definitie

De *Möbius functie* μ, naar A. Möbius (1790–1868), is een functie van $\mathbb{N}^*$ naar de verzameling $\{-1, 0, +1\}$ die als volgt gedefinieerd wordt:

$$\mu(d) = \begin{cases} 1 & \text{als } d = 1 \\ (-1)^r & \text{als } d \text{ een product is van } r \text{ verschillende priemgetallen} \\ 0 & \text{als } d \text{ een meervoudige priemfactor bezit.} \end{cases}$$

6.4.2 Een eerste eigenschap

Stelling 6.4.1. *Voor elk natuurlijk getal $n \geq 2$ zal de som van de waarden $\mu(d)$, genomen over alle delers van n, gelijk zijn aan 0; m.a.w.*

$$\sum_{d|n} \mu(d) = 0.$$

Bewijs. Veronderstel dat $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Elke deler d is dan van de vorm $d = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}$ met $0 \leq x_i \leq e_i$. Bovendien is $\mu(d) = 0$ tenzij elk van de x_i $(1 \leq i \leq k)$ gelijk is aan 0 of 1. Bijgevolg zal elke deler d waarvoor $\mu(d) \neq 0$, corresponderen met een deelverzameling van $\{p_1, p_2, \dots, p_k\}$ bestaande uit de priemgetallen p_i met $x_i = 1$. Het aantal dergelijke deelverzamelingen van de orde r is $\binom{k}{r}$ en voor elke deler d die het product is van r verschillende priemfactoren geldt dat $\mu(d) = (-1)^r$. Bijgevolg is

$$\sum_{d|n} \mu(d) = 1 - \binom{k}{1} + \binom{k}{2} - \dots + (-1)^k \binom{k}{k} = 0. \qquad \square$$

6.4.3 De Möbius inversieformule

Stelling 6.4.2. *Veronderstel dat g een functie is met definitiegebied (een deelverzameling van) $\mathbb{N}^*$ en dat f een functie is die uit g verkregen wordt door de regel:*

$$f(n) = \sum_{d|n} g(d).$$

Dan kan g omgekeerd verkregen worden uit f door de regel:

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Bewijs. We hebben

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \Bigg(\sum_{c|(n/d)} g(c) \Bigg)$$
$$= \sum \sum \mu(d) g(c).$$

Hierbij wordt de dubbele sommatie genomen over de verzameling S van alle koppels (c, d) waarvoor geldt dat $d \mid n$ en $c \mid (n/d)$. Maar dit is eveneens de verzameling van de koppels (c, d) waarvoor geldt dat $c \mid n$ en $d \mid (n/c)$, zodat we de sommatie als volgt kunnen schrijven:

$$\sum_{c|n} g(c) \Bigg(\sum_{d|(n/c)} \mu(d) \Bigg).$$

Wegens bovenstaande stelling is de som tussen de haken gelijk aan 0 van zodra $n/c \geq 2$. Bijgevolg wordt de bovenstaande uitdrukking

$$g(n) \sum_{d|1} \mu(d) = g(n)\mu(1) = g(n),$$

wat te bewijzen was. □

Gevolg

Aangezien $\sum_{d|n} \Phi(d) = n$ zal als gevolg van de Möbius inversieformule

$$\Phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Deze formule is echter niets anders dan een verkorte schrijfwijze van de formule (6.2) die we (in licht aangepaste vorm) herhalen.

$$\Phi(n) = n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k} \right) + \left(\frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \cdots + \frac{n}{p_{k-1} p_k} \right) - \cdots$$
$$\cdots + (-1)^k \left(\frac{n}{p_1 p_2 \cdots p_k} \right).$$

Opmerking

Ook voor de Möbius functie geldt de formule

$$\mu(mn) = \mu(m)\mu(n) \quad \text{voor alle } m, n \in \mathbb{N}^* \text{ met } \gcd(m, n) = 1.$$

Oefeningen

1. Bepaal $\Phi(1992)$.

2. Bewijs dat voor elke twee natuurlijke getallen geldt:

$$\Phi(n^m) = n^{m-1}\Phi(n).$$

3. Bewijs dat voor een gegeven natuurlijk getal n de som van al de natuurlijke getallen $x \in \mathbb{N}[1, n]$ die copriem zijn met n gelijk is aan $\frac{1}{2}n\Phi(n)$.

4. Voor een natuurlijk getal definiëren we

$$\sigma(n) := \sum_{d|n} d.$$

   (a) Geef een formule voor $\sigma(n)$ als $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

   (b) Vereenvoudig

$$\sum_{d|n} \mu(d)\, \sigma\Big(\frac{n}{d}\Big).$$

Hoofdstuk 7

Modulo rekenen

7.1 Congruenties

Veronderstel dat x_1 en x_2 gehele getallen zijn en dat m een positief natuurlijk getal is. We noemen dan x_1 en x_2 *congruent modulo* m dan en slechts dan als $x_1 - x_2$ deelbaar is door m. We noteren dit als

$$x_1 \equiv x_2 \pmod{m}.$$

Het is eenvoudig na te gaan dat de relatie *congruent modulo* m voor vaste m, een equivalentierelatie is. De equivalentieklassen worden de *congruentieklassen modulo* m genoemd. We zeggen ook soms dat x_1 en x_2 *equivalent zijn modulo* m. Twee gehele getallen zijn congruent modulo m dan en slechts dan als ze dezelfde rest opleveren na deling door m. Met andere woorden x_1 en x_2 zijn congruent modulo m dan en slechts dan als er een geheel getal t bestaat zodanig dat

$$x_1 = x_2 + mt.$$

De congruentieklassen modulo m worden daarom ook nog *de restklassen modulo* m genoemd, en de klasse met representant r, wordt soms genoteerd door $[r]_m$ of kortweg door $[r]$ indien er geen verwarring mogelijk is. De verzameling van de restklassen modulo m (met andere woorden de quotiëntverzameling van $\mathbb{Z}$ met betrekking tot de equivalentierelatie congruent modulo m) wordt genoteerd door $\mathbb{Z}/m$. Indien we uit elke restklasse de kleinste natuurlijke representant kiezen, dan ontstaat de verzameling $\mathbb{N}[0, m-1]$. Er bestaat m.a.w. een bijectie tussen de verzamelingen $\mathbb{Z}/m$ en $\mathbb{N}[0, m-1]$.

Stelling 7.1.1. *Veronderstel dat m een positief natuurlijk getal is en dat x_1, x_2, y_1, y_2 gehele getallen zijn zodanig dat*

$$x_1 \equiv x_2 \pmod{m}, \quad y_1 \equiv y_2 \pmod{m}.$$

Dan gelden volgende eigenschappen:

(1) $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,

(2) $x_1 y_1 \equiv x_2 y_2 \pmod{m}$.

Bewijs. (1) Uit het gegeven volgt dat er gehele getallen t en t' bestaan zodanig dat

$$x_1 - x_2 = mt, \qquad y_1 - y_2 = mt'.$$

Bijgevolg geldt

$$\begin{aligned}(x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2)\\ &= mt + mt'\\ &= m(t + t').\end{aligned}$$

Bijgevolg zijn $x_1 + y_1$ en $x_2 + y_2$ congruent modulo m.

(2) Merk op dat

$$\begin{aligned}x_1y_1 - x_2y_2 &= (x_1 - x_2)y_1 + x_2(y_1 - y_2)\\ &= mty_1 + x_2mt'\\ &= m(y_1t + x_2t').\end{aligned}$$

Bijgevolg zijn x_1y_1 en x_2y_2 congruent modulo m. □

De negenproef

Veronderstel dat $(x_nx_{n-1}\dots x_2x_1x_0)_{10}$ *de voorstelling is van het getal* x *in basis* 10. *Bewijs dan dat*

$$x \equiv \sum_{i=0}^{n} x_i \pmod 9.$$

Oplossing.
Uit de definitie van de voorstelling van een getal in basis 10, volgt dat

$$\begin{aligned}x - (\sum_{i=0}^{n} x_i) &= \sum_{i=0}^{n} x_i(10)^i - \sum_{i=0}^{n} x_i\\ &= \sum_{i=1}^{n}((10)^i - 1)x_i.\end{aligned}$$

Aangezien nu voor elk natuurlijk getal $i \geq 1$ geldt dat $((10)^i - 1)$ deelbaar is door 9, volgt hieruit de gevraagde congruentie.

Indien we nu kort $\theta(x)$ schrijven voor $\sum_{i=0}^{n} x_i$, dan hebben we dus aangetoond dat $\theta(x) \equiv x \pmod 9$. Bijgevolg geldt wegens stelling 7.1.1

$$\theta(x)\theta(y) \equiv xy \pmod 9.$$

We hebben eveneens dat

$$\theta(xy) \equiv xy \pmod 9,$$

zodat

$$\theta(xy) \equiv \theta(x)\theta(y) \pmod 9.$$

Dit is de gekende *negenproef* voor de vermenigvuldiging van gehele getallen. Als bijvoorbeeld $x = 12$ en $y = 13$, is $\theta(x) = 3$, $\theta(y) = 4$, $\theta(x)\theta(y) = 12$, $xy = 156$ en $\theta(xy) = 12$. We hebben nu dat $\theta(xy) \equiv \theta(x)\theta(y) \equiv 3 \pmod 9$.

7.2 Optelling en vermenigvuldiging in $\mathbb{Z}/m$

We zullen nu in de verzameling $\mathbb{Z}/m$ een optelling $\oplus$ en een vermenigvuldiging $\otimes$ definiëren.

$$[x]_m \oplus [y]_m = [x + y]_m$$
$$[x]_m \otimes [y]_m = [x \cdot y]_m.$$

Merk op dat de bewerkingen $+$ en $\cdot$ de optelling en de vermenigvuldiging zijn van gehele getallen, terwijl $\oplus$ en $\otimes$ bewerkingen definiëren met deelverzamelingen van gehele getallen. Opdat de definitie zinvol zou zijn, moeten we er ons van vergewissen dat deze definitie onafhankelijk is van de keuze van de representanten x en y uit de klassen $[x]_m$ en $[y]_m$. Met andere woorden, als $[x]_m$ en $[x']_m$ dezelfde klasse voorstellen en als $[y]_m$ en $[y']_m$ dezelfde klasse voorstellen, dan moeten ook $[x]_m \oplus [y]_m$ en $[x']_m \oplus [y']_m$ dezelfde klasse voorstellen, analoog moet dit ook gelden voor de vermenigvuldiging. Dat dit wel degelijk het geval is, volgt onmiddellijk uit Stelling 7.1.1.

De eigenschappen die voor de optelling en de vermenigvuldiging van restklassen modulo m gelden, zijn dan ook een onmiddellijk gevolg van de eigenschappen voor de optelling en de vermenigvuldiging van de gehele getallen, zoals we die samengevat hebben in paragraaf 2.1.2. We hernemen deze eigenschappen, maar nu voor de restklassen modulo m.

Voor alle $[a]_m, [b]_m, [c]_m \in \mathbb{Z}/m$ geldt:

(A1) $[a]_m \oplus [b]_m \in \mathbb{Z}/m$ en $[a]_m \otimes [b]_m \in \mathbb{Z}/m$.

(A2) $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$ en $[a]_m \otimes [b]_m = [b]_m \otimes [a]_m$.

(A3) $([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$ en
$([a]_m \otimes [b]_m) \otimes [c]_m = [a]_m \otimes ([b]_m \otimes [c]_m)$.

(A4) $[a]_m \oplus [0]_m = [a]_m$ en $[a]_m \otimes [1]_m = [a]_m$.

(A5) $[a]_m \otimes ([b]_m \oplus [c]_m) = ([a]_m \otimes [b]_m) \oplus ([a]_m \otimes [c]_m)$.

(A6) Er bestaat een $-[a]_m = [-a]_m \in \mathbb{Z}/m : [a]_m \oplus (-[a]_m) = [0]_m$.

Merk echter op dat de schrappingswet voor de vermenigvuldiging (zie **(A7)** in 2.1.2) in $\mathbb{Z}/m$ niet geldt. Zo is bijvoorbeeld in $\mathbb{Z}/6$,

$$[3]_6 \otimes [1]_6 = [3]_6 \otimes [5]_6,$$

en alhoewel $[3]_6 \neq [0]_6$ mogen we de klasse $[3]_6$ niet schrappen, want $[1]_6 \neq [5]_6$.

Ook kan het voorkomen dat $[a]_m \otimes [b]_m = [0]_m$ terwijl nochtans $[a]_m \neq [0]_m$ en $[b]_m \neq [0]_m$, dergelijk geval doet zich namelijk voor indien a en b echte delers zijn van m en m een deler is van ab. Zo is bijvoorbeeld in $\mathbb{Z}/6$,

$$[3]_6 \otimes [2]_6 = [0]_6.$$

Men zegt daarom dat de klassen $[a]_m$ met a een echte deler van m, *nuldelers* zijn in $\mathbb{Z}/m$. Indien $m = p$ een priemgetal is, dan bezit $\mathbb{Z}/p$ dus geen nuldelers.

Opmerking

Indien er geen verwarring mogelijk is, zullen we in het vervolg de klassen $[r]_m$ meestal voorstellen door een representant $r+tm$ en zullen we voor de optelling van twee klassen in plaats van $[a]_m \oplus [b]_m$, de notatie $a+b \pmod m$ gebruiken. Analoog zal voor de vermenigvuldiging van twee klassen $[a]_m \otimes [b]_m$ de notatie $a \cdot b \pmod m$ of kortweg $ab \pmod m$ gebruikt worden.

7.3 Inverteerbare elementen in $\mathbb{Z}/m$

Een geheel getal r ($r \neq \pm 1$) bezit geen invers element in $\mathbb{Z}$ voor de vermenigvuldiging. In $\mathbb{Z}/m$ is de situatie enigszins anders. We gaan na wanneer een element van $\mathbb{Z}/m$ een invers element in $\mathbb{Z}/m$ bezit.

Definitie

Een element $r \in \mathbb{Z}/m$ wordt *inverteerbaar* genoemd als er een element x in $\mathbb{Z}/m$ bestaat, zodanig dat $rx = 1$ in $\mathbb{Z}/m$, met andere woorden indien $rx \equiv 1 \pmod m$. We noteren het *invers element* x van r als r^{-1}.

Stelling 7.3.1. *Een element r in $\mathbb{Z}/m$ is inverteerbaar dan en slechts dan als r en m onderling ondeelbaar zijn. In het bijzonder is in $\mathbb{Z}/p$, p een priemgetal, elk element verschillend van 0 inverteerbaar.*

Bewijs. Veronderstel dat r inverteerbaar is, dan bestaat er een geheel getal x, zodanig dat $rx \equiv 1 \pmod{m}$. Bijgevolg bestaat er een $k \in \mathbb{Z}$ zodanig dat $rx - 1 = km$, of

$$rx - km = 1.$$

Elke gemene deler van r en van m is dus bijgevolg ook een deler van 1, of met andere woorden $\gcd(r, m) = 1$.

Omgekeerd, veronderstel dat r en m onderling ondeelbaar zijn, dan bestaan er gehele getallen x en y, zodanig dat $rx + my = 1$ (zie Stelling 6.2.1), hetgeen gelijkwaardig is met $xr \equiv 1 \pmod{m}$. □

Opmerking

Het bewijs van deze stelling geeft een expliciete methode om het invers van een gegeven element modulo m te bepalen. Bijvoorbeeld, veronderstel dat we het invers van 5 (mod 18) willen bepalen. Dan gebruiken we de Stelling van Bézout (Stelling 6.2.1) om 1 te schrijven als lineaire combinatie van 5 en 18, en we vinden $1 = 2 \cdot 18 - 7 \cdot 5$; hieruit halen we dat $(-7) \cdot 5 \equiv 1 \pmod{18}$ of dus $11 \cdot 5 \equiv 1 \pmod{18}$.

Gevolgen

Merk op dat we in 6.3, $\Phi(m)$ gedefinieerd hebben als het aantal gehele getallen r, met $1 \leq r \leq m$, die copriem zijn met m. Het aantal inverteerbare elementen in $\mathbb{Z}/m$ is bijgevolg gelijk aan $\Phi(m)$.

De volgende stelling is één van de klassiekers in de elementaire getaltheorie en heeft een groot aantal toepassingen.

Stelling 7.3.2 (Stelling van Euler)**.** *Als* $\gcd(y, m) = 1$*, dan geldt*

$$y^{\Phi(m)} \equiv 1 \pmod{m}.$$

Bewijs. Aangezien $\gcd(y, m) = 1$, is y inverteerbaar in $\mathbb{Z}/m$. Noem $(\mathbb{Z}/m)^\times$ de verzameling van de inverteerbare elementen in $\mathbb{Z}/m$; bijgevolg is $y \in (\mathbb{Z}/m)^\times$. We weten dat $|(\mathbb{Z}/m)^\times| = \Phi(m)$; stel dus

$$(\mathbb{Z}/m)^\times = \{u_1, u_2, \ldots, u_{\Phi(m)}\}.$$

Merk op dat de verzameling $(\mathbb{Z}/m)^\times$ gesloten[1] is onder vermenigvuldiging en onder inverteren, zodat de afbeelding

$$\alpha\colon (\mathbb{Z}/m)^\times \to (\mathbb{Z}/m)^\times\colon x \mapsto yx$$

een bijectie is. Bijgevolg is

$$\begin{aligned} y(\mathbb{Z}/m)^\times &= \{yu_1, yu_2, \ldots, yu_{\Phi(m)}\} \\ &= \{u_1, u_2, \ldots, u_{\Phi(m)}\} = (\mathbb{Z}/m)^\times. \end{aligned}$$

Stel nu u gelijk aan het product modulo m van alle elementen uit $(\mathbb{Z}/m)^\times$, m.a.w.

$$u \equiv \prod_{i=1}^{\Phi(m)} u_i \pmod{m}.$$

Aangezien $y(\mathbb{Z}/m)^\times = (\mathbb{Z}/m)^\times$ is

$$u \equiv \prod_{i=1}^{\Phi(m)} u_i \equiv \prod_{i=1}^{\Phi(m)} yu_i \equiv y^{\Phi(m)}u \pmod{m}.$$

Aangezien u als product van al de inverteerbare elementen in $\mathbb{Z}/m$ eveneens inverteerbaar is, kunnen we de schrappingswet toepassen, zodat $y^{\Phi(m)} \equiv 1 \pmod{m}$. □

Gevolg

In het bijzonder geval dat $m = p$ een priemgetal is, en dus $\Phi(p) = p - 1$, wordt de stelling van Euler:

$$\text{Als } p \nmid y, \text{ dan is } y^{p-1} \equiv 1 \pmod{p}.$$

Deze vorm is beter gekend onder de naam *kleine stelling van Fermat*. Het is opmerkelijk dat Fermat dit resultaat zonder bewijs publiceerde in 1640, terwijl het maar pas rond 1760 als bijzonder geval door Euler werd bewezen.

Toepassing

Toon aan dat voor elk positief natuurlijk getal n en elk priemgetal p geldt dat $n^p \equiv n \pmod{p}$. Bewijs hieruit dat n en n^5 steeds op hetzelfde cijfer eindigen.

[1] Hiermee bedoelen we dat het product van twee elementen in $(\mathbb{Z}/m)^\times$ opnieuw in $(\mathbb{Z}/m)^\times$ zit, en dat het inverse van een element van $(\mathbb{Z}/m)^\times$ (dat steeds bestaat) weer in $(\mathbb{Z}/m)^\times$ zit. Dit drukt in feite uit dat $(\mathbb{Z}/m)^\times$ een *groep* vormt; zie Hoofdstuk 8 verderop.

Oplossing.
Indien $p \nmid n$, dan volgt uit de stelling van Fermat dat $n^{p-1} \equiv 1 \pmod{p}$ en dus dat $n^p \equiv n \pmod{p}$. Anderzijds, indien $p \mid n$, dan zijn zowel n als n^p veelvouden van p.

Indien we nu dit resultaat toepassen in het geval $p = 5$, dan volgt hieruit dat $n^5 - n$ deelbaar is door 5. Anderzijds is $n^5 - n = n(n-1)(n^3+n^2+n+1)$ en dus ook even. Hieruit volgt dat $n^5 - n$ deelbaar is door 5 en door 2, bijgevolg door 10, zodat n en n^5 op hetzelfde cijfer eindigen.

7.4 Lineaire congruenties

Na de definitie van congruentie te hebben gegeven, is het logisch dat we proberen vergelijkingen op te lossen in $\mathbb{Z}/m$. We zullen ons beperken tot de lineaire vergelijkingen.

Definities

Een vergelijking van de vorm $ax \equiv b \pmod{m}$ met a en b gegeven gehele getallen, en x een onbekende in $\mathbb{Z}/m$, wordt een *lineaire congruentie* genoemd. Het oplossen van een dergelijke lineaire congruentie is gelijkwaardig met het zoeken naar een koppel $(x, t), x \in \mathbb{N}[0, m-1], t \in \mathbb{Z}$, zodanig dat $ax = b + mt$.

Merk op dat $ax \equiv b \pmod{m}$ in feite een verkorte schrijfwijze is voor $[a]_m \otimes [x]_m = [b]_m$. Een oplossing van deze vergelijking tussen congruentieklassen modulo m is dus zelf een congruentieklasse modulo m. We zullen echter ook nu weer spreken van de oplossing r i.p.v. $[r]_m$. Met deze afspraken zijn twee oplossingen r_1 en r_2 van eenzelfde lineaire congruentie verschillend dan en slechts dan als $[r_1]_m \neq [r_2]_m$.

Stelling 7.4.1. (1) *Als* $d = \gcd(a, m) \nmid b$, *dan bezit* $ax \equiv b \pmod{m}$ *geen oplossing.*

(2) *Als* $d = \gcd(a, m) \mid b$, *dan bezit* $ax \equiv b \pmod{m}$ *juist* d *oplossingen* r *waarbij* $r \in \mathbb{N}[0, m-1]$.

Bewijs. (1) Veronderstel dat $\gcd(a, m) = d > 1$ geen deler is van b. Indien $r \in \mathbb{N}[0, m-1]$ een oplossing is van de lineaire congruentie $ax \equiv b \pmod{m}$, dan bestaat er een geheel getal k zodanig dat $ar - b = km$ of dus zodanig dat $ar - km = b$. Hieruit zou volgen dat d een deler is van b. Een tegenstrijdigheid.

(2) Veronderstel dat $\gcd(a, m) = 1$, dan is a inverteerbaar in $\mathbb{Z}/m$ wegens Stelling 7.3.1. Bijgevolg bestaat er een element $a^{-1} \in \mathbb{Z}/m$ zo-

danig dat $aa^{-1} \equiv 1 \pmod{m}$; hieruit volgt dat de vergelijking $ax \equiv b \pmod{m}$ equivalent is met $a^{-1}(ax) \equiv a^{-1}b \pmod{m}$ of dus met $x \equiv a^{-1}b \pmod{m}$. Veronderstel nu dat $\gcd(a, m) = d > 1$ en dat $d \mid b$. We kunnen dan de beide leden van de lineaire congruentie delen door d en we bekomen dan

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}, \quad \gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1.$$

Deze laatste lineaire congruentie bezit juist één oplossing r in $\mathbb{N}[0, \frac{m}{d} - 1]$. Alle oplossingen van $ax \equiv b \pmod{m}$ zijn bijgevolg van de gedaante $r + t\frac{m}{d}, t \in \mathbb{N}[0, d - 1]$. Er zijn dus juist d oplossingen. □

Opmerkingen

1. Veronderstel dat $\gcd(a, m) = 1$, dan bezit $ax \equiv b \pmod{m}$ juist één oplossing. Wegens het algoritme van Euclides (zie Stelling 6.2.1), weten we dat er gehele getallen r en s bestaan zodanig dat $ar + ms = 1$, en bijgevolg is dan $a(rb) + m(sb) = b$ of $a(rb) \equiv b \pmod{m}$. Hieruit volgt dat $rb \pmod{m}$ een oplossing is van de gegeven lineaire congruentie.

2. In de praktijk kunnen we de oplossing het gemakkelijkst op de volgende manier vinden. We controleren eerst of $d = \gcd(a, m)$ een deler is van b die groter is dan 1. Indien dit het geval is, dan moeten we eerst d wegdelen in de congruentie. Veronderstel dat dit gebeurd is, dan schrijven we de lineaire congruentie $ax \equiv b \pmod{m}$ in de vorm $ax \equiv (b + tm) \pmod{m}$ met $b + tm$ een veelvoud van a. De oplossing van de lineaire congruentie is dan van de vorm $\dfrac{b + tm}{a} \pmod{m}$.

Voorbeelden

Zoek de oplossing(en) van de volgende lineaire congruenties.

1. $4x \equiv 1 \pmod{15}$. Dit is gelijkwaardig met $4x \equiv 16 \pmod{15}$ en bijgevolg is $x \equiv 4 \pmod{15}$.

2. $14x \equiv 27 \pmod{31}$. Dit is gelijkwaardig met $14x \equiv 58 \pmod{31}$ en dus met $7x \equiv 29 \pmod{31}$, hetgeen op zijn beurt gelijkwaardig is met $7x \equiv 91 \pmod{31}$, zodat $x \equiv 13 \pmod{31}$.

3. $6x \equiv 15 \pmod{33}$. Aangezien $\gcd(6, 33) = 3$ en 3 een deler is van 15, zijn er 3 oplossingen in $\mathbb{N}[0, 32]$. We delen de congruentie door 3, en we zoeken de oplossing van $2x \equiv 5 \pmod{11}$. Dit is gelijkwaardig met

$2x \equiv 16 \pmod{11}$ of met $x \equiv 8 \pmod{11}$. Alle oplossingen modulo 33, zijn dus van de gedaante $8+11t,\ t \in \{0,1,2\}$. Bijgevolg is x congruent met $8, 19, 30$ modulo 33.

Toepassing

Zoek de oplossingen $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ *van* $9x + 16y = 35$.

Oplossing.
De vergelijking $9x + 16y = 35$ impliceert dat x en y oplossingen zijn van het stelsel lineaire congruenties

$$\begin{cases} 9x \equiv 35 \pmod{16} \\ 16y \equiv 35 \pmod{9}. \end{cases}$$

We lossen één van de congruenties op en substitueren de oplossing dan in de andere lineaire congruentie, bijvoorbeeld:

$$\begin{aligned} & 16y \equiv 35 \pmod{9} \\ \iff\ & 7y \equiv 35 \pmod{9} \\ \iff\ & y \equiv 5 \pmod{9} \\ \iff\ & y = 5 + 9t, \quad t \in \mathbb{Z}. \end{aligned}$$

Indien we deze oplossing nu substitueren in de gegeven vergelijking, dan bekomen we $9x + 16(5 + 9t) = 35$ hetgeen impliceert dat $x = -5 - 16t$.

Opmerkingen

1. In plaats van de oplossing $y = 5+9t$ van de lineaire congruentie $16y \equiv 35 \pmod{9}$ te substitueren in $9x + 16y = 35$ en dan op te lossen naar x, hadden we ook de andere lineaire congruentie $9x \equiv 35 \pmod{16}$ onafhankelijk kunnen oplossen. Deze congruentie heeft als oplossing $x \equiv -5 \pmod{16}$, bijgevolg bestaat $t' \in \mathbb{Z}$ zodanig dat $x = -5 + 16t'$. De substitutie van $y = 5+9t$ en $x = -5+16t'$ in de gegeven vergelijking levert dan $t = -t'$. Deze werkwijze heeft als voordeel dat we de twee lineaire congruenties parallel kunnen uitrekenen.

2. Elke vergelijking $ax + by = c$ in $\mathbb{Z}$ (a, b en c gehele getallen), wordt *een lineaire diophantische vergelijking met 2 onbekenden* genoemd.

7.5 De stelling van Wilson en toepassingen

Stelling 7.5.1 (Stelling van Wilson)**.** *Als p een priemgetal is, dan geldt*

$$(p-1)! \equiv -1 \pmod{p}.$$

Bewijs. We merken vooreerst op dat de stelling triviaal voldaan is voor $p = 2$. Veronderstel daarom nu dat p een oneven priemgetal is. We beschouwen de verzameling $\mathbb{Z}/p \setminus \{0\}$. Aangezien p een priemgetal is, zal elk element a van deze verzameling inverteerbaar zijn en het invers element a^{-1} behoort eveneens tot deze verzameling. Bijgevolg kunnen we bij de berekening van $(p-1)!$ modulo p telkens een element a samennemen met zijn invers element a^{-1}, (en $aa^{-1} \equiv 1 \pmod{p}$) op voorwaarde dat $a \not\equiv a^{-1} \pmod{p}$. Maar $a \equiv a^{-1} \pmod{p}$ dan en slechts dan als $(a^2 - 1) \equiv 0 \pmod{p}$, zodat dus p een deler is van $a^2 - 1 = (a+1)(a-1)$. Aangezien p een priemgetal is, volgt hieruit dat p ofwel een deler is van $a - 1$ of van $a + 1$. Aangezien $a \in \mathbb{N}[1, p-1]$, volgt hieruit dat ofwel $a = 1$ ofwel $a = p - 1$. Bijgevolg is

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (1)^{\frac{p-3}{2}} \equiv -1 \pmod{p}. \qquad \square$$

Stelling 7.5.2. *Veronderstel dat p een oneven priemgetal is, dan bestaat er een $a \in \mathbb{Z}/p$ waarvoor $a^2 \equiv -1 \pmod{p}$ dan en slechts dan als $p \equiv 1 \pmod{4}$.*

Bewijs. Merk op dat

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \\ &\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right) \cdot \left((-\frac{p-1}{2}) \cdot (-\frac{p-3}{2}) \cdots (-1)\right) \pmod{p} \\ &\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \cdot (-1)^{\frac{p-1}{2}} \pmod{p}.\end{aligned}$$

Deze congruentie is verkregen door van elk van de factoren van $\frac{p+1}{2}$ tot $p-1$ (zo zijn er $\frac{p-1}{2}$) telkens p af te trekken.

Anderzijds is wegens de stelling van Wilson, $(p-1)! \equiv -1 \pmod{p}$. Indien $\frac{p-1}{2}$ even is, bijvoorbeeld $\frac{p-1}{2} = 2k$, zodat $p = 4k + 1$, dan is

$$(p-1)! \equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \equiv -1 \pmod{p}.$$

Met andere woorden, $a = \frac{p-1}{2}!$ heeft de eigenschap dat $a^2 \equiv -1 \pmod{p}$ als $p \equiv 1 \pmod{4}$.

Veronderstel nu omgekeerd dat er een a bestaat zodanig dat $a^2 \equiv -1 \pmod{p}$, dan zal eveneens $(-a)^2 \equiv -1 \pmod{p}$. Merk bovendien op dat uit $a^2 \equiv b^2 \pmod{p}$ eenvoudig volgt dat $a \equiv \pm b \pmod{p}$, zodat $x = a$ en $x = -a$ de enige waarden zijn waarvoor $x^2 \equiv -1 \pmod{p}$. Met elk element $t \in \mathbb{Z}/p \setminus \{0, a, -a\}$ correspondeert juist één element $t' \in \mathbb{Z}/p \setminus \{0, a, -a\}$, $t \neq t'$, zodanig dat $tt' \equiv -1 \pmod{p}$. Hieruit volgt dat

$$\begin{aligned}(p-1)! &\equiv -1 \pmod{p} \\ &\equiv (-1)^{\frac{p-3}{2}} \cdot a \cdot (-a) \pmod{p} \\ &\equiv (-1)^{\frac{p-3}{2}} \pmod{p}.\end{aligned}$$

Aangezien wegens de stelling van Wilson, $(p-1)! \equiv -1 \pmod{p}$, volgt hieruit dat $\frac{p-3}{2}$ oneven is, bijvoorbeeld $\frac{p-3}{2} = 2k-1$, zodat $p = 4k+1$. □

7.6 Stelsels lineaire congruenties

We beschouwen nu een stelsel van lineaire congruenties, met andere woorden een stelsel van de gedaante

$$a_i x \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k \quad \gcd(a_i, m_i) \mid b_i.$$

Merk op dat we er steeds voor kunnen zorgen dat de vergelijkingen in dit stelsel van de vorm $x \equiv b_i \pmod{m_i}$ met $b_i \in \mathbb{N}[0, m_i - 1]$ zijn (zie oplossen van lineaire congruenties). We zullen ons daarom beperken tot de stelsels van de vorm

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}[0, m_i - 1], i = 1, \ldots, k.$$

Voorbeeld

Zoek een oplossing van het volgende stelsel lineaire congruenties

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7}. \end{cases}$$

Oplossing.
Uit de eerste lineaire congruentie volgt dat $x = 1 + 3k_1$. Indien we dit substitueren in de tweede lineaire congruentie, dan is $1 + 3k_1 \equiv 2 \pmod{5}$ hetgeen impliceert dat $3k_1 \equiv 1 \pmod{5}$ of dat $k_1 \equiv 2 \pmod{5}$. Bijgevolg is

$k_1 = 2 + 5k_2$, zodat $x = 7 + 15k_2$. We substitueren dit nu in de derde lineaire congruentie: $7 + 15k_2 \equiv 3 \pmod 7$, of dus $15k_2 \equiv -4 \pmod 7$, hetgeen gelijkwaardig is met $15k_2 \equiv 3 \pmod 7$. Hieruit volgt dat $5k_2 \equiv 1 \pmod 7$ of dus $k_2 \equiv 3 \pmod 7$. Elke oplossing x van het stelsel is met andere woorden van de vorm $x = 7 + 15(3 + 7k_3) = 52 + 105k_3$, zodat $x \equiv 52 \pmod{105}$.

Opmerking

Het zoeken van de oplossing is volgens de bovenstaande methode vrij omslachtig. Het wordt vooral veel rekenwerk indien er meerdere congruenties in het stelsel voorkomen. Merk op dat dit stelsel een unieke oplossing bezit modulo 105, omdat 3, 5 en 7 onderling ondeelbaar zijn. In de volgende stelling zullen we dit algemeen bewijzen. We zullen bovendien een veel sneller algoritme opstellen om dergelijke stelsels van lineaire congruenties op te lossen. De stelling wordt gemeenzaam de *Chinese reststelling* genoemd omdat het voorbeeld van hierboven reeds in een Chinees wiskundeboek uit de 4de eeuw besproken werd.

Stelling 7.6.1 (Chinese reststelling)**.** *Veronderstel dat $m_1, \ldots, m_k$ natuurlijke getallen zijn die twee aan twee onderling ondeelbaar zijn, m.a.w. voor elke $i \neq j$ geldt* $\gcd(m_i, m_j) = 1$. *Zij $M = \prod_{i=1}^{k} m_i = m_1 \cdots m_k$. Beschouw verder voor elke i een $b_i \in \mathbb{N}[0, m_i - 1]$. Dan heeft het stelsel lineaire congruenties*

$$x \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k$$

juist 1 oplossing modulo M.

Bewijs. Beschouw de afbeelding

$$\theta\colon \begin{array}{c} \mathbb{Z}/M \to \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_k\colon \\ t \bmod M \mapsto (t \bmod m_1, \ldots, t \bmod m_k). \end{array}$$

Vooreerst gaan we na dat deze afbeelding *goed gedefinieerd* is, d.w.z. dat de uitdrukking $(t \bmod m_1, \ldots, t \bmod m_k)$ onafhankelijk is van de keuze van de representant $t \in \mathbb{Z}$ voor het element $t \bmod M \in \mathbb{Z}/M$. Inderdaad, veronderstel dat $s \equiv t \pmod M$; dan is $M \mid s - t$, en bijgevolg is $m_i \mid s - t$ voor elke i, zodat ook $s \equiv t \pmod{m_i}$ voor elke i.

Vervolgens gaan we na dat deze afbeelding *injectief* is. Inderdaad, veronderstel dat $s, t \in \mathbb{Z}$ zodanig zijn dat $\theta(s \bmod M) = \theta(t \bmod M)$. Dan is $s \equiv t \pmod{m_i}$ voor elke $i \in \{1, \ldots, k\}$, en dus $m_i \mid s - t$ voor elke i. Omdat de m_i onderling ondeelbaar zijn, volgt uit Stelling 6.2.2(3) nu dat $M \mid s - t$, en dus is $s \equiv t \pmod M$. Hieruit volgt dat θ injectief is.

Merk nu op dat $\mathbb{Z}/M$ en $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_k$ even veel elementen bevatten (namelijk M). Een injectie tussen twee verzamelingen die dezelfde eindige kardinaliteit hebben, is echter noodzakelijk een bijectie, en dus besluiten we dat θ een bijectie is.

In het bijzonder is er juist één element $t \bmod M$ waarvoor

$$\theta(t \bmod M) = (b_1 \bmod m_1, \ldots, b_k \bmod m_k),$$

en dat is precies wat we wilden bewijzen. □

Het algoritme

We leggen het algoritme eerst uit aan de hand van ons voorbeeld.

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7. \end{cases}$$

We zoeken een oplossing van de vorm

$$x = y_1 \cdot (5 \cdot 7) + y_2 \cdot (3 \cdot 7) + y_3 \cdot (3 \cdot 5)\,. \tag{7.1}$$

De getallen tussen haakjes achter y_i zijn de producten van al de moduli uitgezonderd de modulus m_i uit de i-de congruentie. Indien we nu deze gedaante van x invullen in de achtereenvolgende congruenties, dan ontstaat een stelsel van congruenties in y_i, namelijk:

$$\begin{cases} 35y_1 \equiv 1 \pmod 3 \\ 21y_2 \equiv 2 \pmod 5 \\ 15y_3 \equiv 3 \pmod 7. \end{cases}$$

Deze drie congruenties kunnen nu elk afzonderlijk opgelost worden, eventueel met behulp van Stelling 7.4.1. We vinden hier de oplossing

$$\begin{cases} y_1 \equiv 2 \pmod 3 \\ y_2 \equiv 2 \pmod 5 \\ y_3 \equiv 3 \pmod 7. \end{cases}$$

Substitueren we de waarden $y_1 = 2, y_2 = 2, y_3 = 3$ in (7.1), dan bekomen we $x = 157$, hetgeen dan modulo $105 = (3 \cdot 5 \cdot 7)$ congruent is met 52.

Algemeen bestaat het algoritme voor het oplossen van het stelsel

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}[0, m_i - 1],\ i = 1, \ldots, k$$

erin een oplossing te zoeken van de vorm

$$x = \sum_{i=1}^{k} m^{(i)} y_i, \quad \text{met} \;\; m^{(i)} = \frac{\prod_{j=1}^{k} m_j}{m_i}.$$

Het stelsel herleidt zich dan tot een stelsel van de vorm

$$m^{(i)} y_i \equiv b_i \pmod{m_i}, \quad y_i \in \mathbb{N}[0, m_i - 1], \; i = 1, \ldots, k.$$

Elk van deze lineaire congruenties uit het stelsel kan door middel van Stelling 7.4.1 opgelost worden. (Merk op dat er altijd een unieke oplossing is van deze lineaire congruentie, precies omdat $\gcd(m^{(i)}, m_i) = 1$.) Na substitutie vinden we de gezochte waarde van x.

Opmerking

Indien het stelsel slechts uit 2 congruenties bestaat, dan is $x = m_2 y_1 + m_1 y_2$.

7.7 Primitieve wortels

7.7.1 De orde van een element modulo m

Veronderstel dat $a \in \mathbb{Z} \setminus \{0\}$, $m \in \mathbb{N} \setminus \{0\}$ en dat $\gcd(a, m) = 1$. De verzameling $\{s \in \mathbb{N} \mid a^s \equiv 1 \pmod{m}\}$ is niet ledig, want wegens de stelling van Euler (Stelling 7.3.2) is

$$a^{\Phi(m)} \equiv 1 \pmod{m}.$$

Bijgevolg bestaat er een kleinste element t in deze verzameling waarvoor dus geldt dat $a^t \equiv 1 \pmod{m}$. We noemen dit natuurlijk getal t de *orde van a modulo m*, en we noteren dit als $t = o_m(a)$. Merk op dat 1 dus altijd de orde 1 heeft.

Voorbeeld

Indien we de opeenvolgende machten van de 10 elementen uit $\mathbb{Z}/11 \setminus \{0\}$ uitrekenen, dan verkrijgen we de volgende tabel.

	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

$a^n \pmod{11}$

Uit deze tabel blijkt onder andere dat de elementen $2, 6, 7$ en 8 orde 10 hebben. Anderzijds hebben $3, 4, 5$ en 9 orde 5, en heeft het element 10 orde 2. Het is geen toeval dat de mogelijke ordes allemaal delers zijn van $10 = \Phi(11)$.

Stelling 7.7.1. *Veronderstel dat* $\gcd(a, m) = 1$*, en stel* $t = o_m(a)$*. Voor alle* $r, s \in \mathbb{Z}$ *geldt:*

(i) $a^s \equiv 1 \pmod{m}$ *als en slechts als* $t \mid s$*;*

(ii) $t \mid \Phi(m)$*;*

(iii) $a^r \equiv a^s \pmod{m}$ *als en slechts als* $r \equiv s \pmod{t}$*.*

Bewijs. (i) Gebruik makend van de Euclidische deling schrijven we

$$s = tq + r \quad \text{met } r \in \mathbb{N}[0, t-1].$$

Merk op dat $t \mid s$ als en slechts als $r = 0$. Omdat $a^t \equiv 1 \pmod{m}$ geldt tevens dat

$$a^s \equiv (a^t)^q \cdot a^r \equiv a^r \pmod{m},$$

en dus is $a^s \equiv 1 \pmod{m}$ als en slechts als $a^r \equiv 1 \pmod{m}$. Omdat $r < t = o_m(a)$ kan dit echter enkel als $r = 0$.

(ii) Uit de stelling van Euler (Stelling 7.3.2) weten we dat $a^{\Phi(m)} \equiv 1 \pmod{m}$. Uit (i) volgt nu onmiddellijk dat $t \mid \Phi(m)$.

(iii) Dit volgt onmiddellijk uit (i). □

7.7.2 Primitieve wortels

Als $a \in \mathbb{Z}/m$, $\gcd(a, m) = 1$, en als de orde van a gelijk is aan $\Phi(m)$, dan wordt a een *primitieve wortel van* m genoemd. Zo zijn bijvoorbeeld $2, 6, 7$ en 8 de primitieve wortels van 11. Niet elk natuurlijk getal m bezit primitieve wortels[2]. Zo zijn $1, 3, 5$ en 7 de $\Phi(8) = 4$ getallen die copriem zijn met 8, maar $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

Stelling 7.7.2. *Als g een primitieve wortel is van m, dan zijn de resten modulo m van $g, g^2, \ldots, g^{\Phi(m)}$ de $\Phi(m)$ natuurlijke getallen uit $\mathbb{N}[1, m-1]$ die copriem zijn met m.*

Bewijs. Aangezien $\gcd(g, m) = 1$, is ook $\gcd(g^k, m) = 1,\ k = 1, \ldots, \Phi(m)$. Bovendien zijn al deze getallen verschillend, want $g^j \equiv g^k \pmod m$ is gelijkwaardig met $j \equiv k \pmod{\Phi(m)}$. □

Voorbeeld

In $\mathbb{Z}/9$ is 2 een primitieve wortel (oefening). Aangezien $\Phi(9) = 6$ zal de verzameling $\{2, 2^2, 2^3, 2^4, 2^5, 2^6\}$ modulo 9, de verzameling zijn van de getallen die copriem zijn met 9. Deze verzameling is inderdaad gelijk aan $\{2, 4, 8, 7, 5, 1\}$.

Stelling 7.7.3. *Zij $\gcd(a, m) = 1$, en stel $t = o_m(a)$. Dan is*

$$o_m(a^k) = \frac{t}{\gcd(k, t)}$$

voor elke $k \in \mathbb{Z}$. In het bijzonder geldt

$$o_m(a^k) = t \iff \gcd(k, t) = 1.$$

Bewijs. Stel $s = o_m(a^k)$, en stel $r = t/\gcd(k, t)$. Merk op dat $kr = \operatorname{lcm}(k, t)$, zodat in het bijzonder $t \mid kr$. Uit Stelling 7.7.1(i) volgt dan dat $a^{kr} \equiv 1 \pmod m$, en dus is $(a^k)^r \equiv 1 \pmod m$, hetgeen impliceert dat $s \mid r$.

Anderzijds volgt uit de definitie van s dat $a^{ks} \equiv 1 \pmod m$, en opnieuw uit Stelling 7.7.1(i) volgt nu dat $t \mid ks$. Omdat uiteraard ook $k \mid ks$ volgt dat $kr = \operatorname{lcm}(k, t) \mid ks$, en bijgevolg $r \mid s$.

We besluiten dat $r = s$, en dit is precies wat we wilden bewijzen. □

[2]Men kan aantonen dat er dan en slechts dan een primitieve wortel van m bestaat als m gelijk is aan 2, 4, p^k of $2p^k$, met p een oneven priemgetal en $k \in \mathbb{N}^*$.

Voorbeeld

We hebben reeds gezien dat het getal 2 de orde 10 bezit, dus een primitieve wortel is van 11. Hieruit volgt dat 2^k met $\gcd(k, 10) = 1$ eveneens primitieve wortels van 11 zijn. Nu is $\gcd(k, 10) = 1$ als en slechts als $k = 1, 3, 7, 9$, en $2^3 \equiv 8 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$ en $2^9 \equiv 6 \pmod{11}$, zodat $2, 6, 7$ en 8 primitieve wortels zijn van 11. We kunnen ons natuurlijk de vraag stellen of er eventueel nog andere primitieve wortels bestaan van 11. We weten uit de vermenigvuldigingstabel van $\mathbb{Z}/11$ dat dit niet het geval is. Dit is eveneens het gevolg van de volgende stelling die we zonder bewijs aannemen.

Stelling 7.7.4. *Elk priemgetal p bezit juist $\Phi(p-1)$ primitieve wortels. Indien g een primitieve wortel is van p, dan is de verzameling*

$$\{g^k \pmod{p} \mid \gcd(k, p-1) = 1\}$$

de verzameling van de primitieve wortels van p.

Zonder bewijs. □

Hoofdstuk 8

Groepen, ringen, lichamen en velden

In Hoofdstuk 2 en Hoofdstuk 7 hebben we de rekenregels opgesomd voor de optelling en de vermenigvuldiging in $\mathbb{Z}$ en in $\mathbb{Z}/m$. We willen in dit hoofdstuk deze regels wat formaliseren; we willen de structuur bepaald door een verzameling en één of meerdere bewerkingen formeel beschrijven.

8.1 Groepen

Een *binaire bewerking* op een verzameling V is een afbeelding van de gedaante

$$f : V \times V \to V : (a, b) \mapsto f(a, b) .$$

Merk dus op dat een binaire bewerking steeds als een gesloten bewerking beschouwd wordt, waarmee we bedoelen dat $f(a, b)$ steeds weer in de oorspronkelijke verzameling V terechtkomt. Naar analogie met de getallenverzamelingen zullen we voor $f(a, b)$ meestal de additieve notatie $(a + b)$ of de multiplicatieve notatie (ab) gebruiken. Er is trouwens geen bezwaar om als voorbeeld steeds de optelling of vermenigvuldiging van (reële) getallen in gedachten te houden. Nochtans moeten we er de aandacht op vestigen dat er heel wat andere bewerkingen in aanmerking komen, zoals we straks met wat voorbeelden zullen illustreren.

Een *groep* is een koppel (G, f), waarbij G een verzameling is en f een binaire bewerking die aan drie bijkomende voorwaarden voldoet. In plaats van (G, f) schrijven we soms ook $(G, \cdot)$ of $(G, +)$, of —als er geen verwarring mogelijk is— kortweg G. Heel vaak zullen we de bewerking ook eenvoudigweg achterwege laten, en dus noteren door het naast elkaar plaatsen van de elementen, zoals we gewoonlijk doen met de vermenigvuldiging; we schrijven dan ab in plaats van $f(a, b)$.

(i) Voor alle $a, b, c \in G$ geldt $a(bc) = (ab)c$ (associatieve wet);

(ii) Er bestaat een $e \in G$ zodat voor alle $a \in G$ geldt dat $ae = ea = a$ (identiteitswet);

(iii) Voor alle $a \in G$ bestaat er een element $a^{-1} \in G$ zodat $aa^{-1} = a^{-1}a = e$ (inversieve wet).

Het element e noemt men *neutraal element*; dit wordt vaak genoteerd als 0 bij additieve notatie, en als 1 bij multiplicatieve notatie.

Het element a^{-1} noemt men het *invers element van* a en wordt bij additieve notatie meestal genoteerd als $-a$ (m.a.w. $a + (-a) = 0$), in dit geval spreken we ook van het *tegengesteld element van* a.

Als G een groep is zodanig dat $ab = ba$ voor alle $a, b \in G$, dan zegt men dat G *commutatief* of *abels* is.

De *orde* van een groep is het aantal elementen van de onderliggende verzameling.

Voorbeelden

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ en $(\mathbb{C}, +)$ zijn abelse groepen voor de gewone optelling, maar $(\mathbb{N}, +)$ is geen groep.

   $(\mathbb{Q}\setminus\{0\}, \cdot)$ is een abelse groep voor de gewone vermenigvuldiging. Analoog zijn $(\mathbb{C}\setminus\{0\}, \cdot)$ en $(\mathbb{R}\setminus\{0\}, \cdot)$ abelse groepen. Anderzijds zijn $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}\setminus\{0\}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ en $(\mathbb{C}, \cdot)$ geen groepen.

2. Stel $G = \{e, a, b, c\}$. We definiëren een binaire bewerking $\bullet$ in G aan de hand van de volgende *bewerkingstabel* of *Cayley tabel*:

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

   De axioma's voor een groep kunnen eenvoudig gecontroleerd worden. Deze groep wordt de *viergroep van Klein* genoemd. In de praktijk moet slechts een gedeelte van de bewerkingstabel gegeven worden en is de rest een gevolg van de gegeven bewerkingen. Zo is het hier voldoende om de volgende zogenaamde *voortbrengende relaties* van de viergroep van Klein op te geven:
   $$a^2 = b^2 = c^2 = abc = 1.$$

3. $(\mathbb{Z}/m, \oplus)$ is een abelse groep, terwijl $(\mathbb{Z}/m\setminus\{0\}, \otimes)$ dan en slechts dan een groep is als m een priemgetal is (oefening). Anderzijds hebben we in het bewijs van Stelling 7.3.2 gezien dat $(Z/m)^\times$, de verzameling van inverteerbare elementen in $\mathbb{Z}/m$, *wel* steeds een groep vormt.

4. De verzameling van de niet-singuliere $(n \times n)$-matrices over $\mathbb{C}$ vormt een groep voor de matrixvermenigvuldiging. Deze groep wordt meestal genoteerd als $\mathsf{GL}(n, \mathbb{C})$ (zie cursus lineaire algebra).

5. De $n!$ permutaties van een verzameling van de orde n vormen een groep voor de samenstelling van permutaties. Deze groep wordt de *symmetrische groep* genoemd, en wordt genoteerd als S_n of als $\mathsf{Sym}(n)$.

6. De groep S_3 is bijvoorbeeld ook de groep van al de transformaties in het Euclidisch vlak die een gelijkzijdige driehoek *abc* afbeeldt op zichzelf. We noemen deze transformaties ook de *symmetrieën* van de gelijkzijdige driehoek. De gelijkzijdige driehoek bezit inderdaad 6 symmetrieën: de identiteit e, de rotatie ρ over 120° in wijzerzin, de rotatie ρ^2 over 240° in wijzerzin (merk op dat $\rho^2 = \rho^{-1}$ eveneens beschouwd kan worden als de rotatie over 120° in tegenwijzerzin), de 3 spiegelingen $\sigma_a, \sigma_b, \sigma_c$ rond de hoogtelijnen door respectievelijk a, b en c. Het is eenvoudig om na te gaan dat de samenstelling van deze symmetrieën gegeven wordt door de volgende Cayley tabel.

$\bullet$	e	ρ	ρ^2	σ_a	σ_b	σ_c
e	e	ρ	ρ^2	σ_a	σ_b	σ_c
ρ	ρ	ρ^2	e	σ_b	σ_c	σ_a
ρ^2	ρ^2	e	ρ	σ_c	σ_a	σ_b
σ_a	σ_a	σ_c	σ_b	e	ρ^2	ρ
σ_b	σ_b	σ_a	σ_c	ρ	e	ρ^2
σ_c	σ_c	σ_b	σ_a	ρ^2	ρ	e

Enkele eenvoudige eigenschappen

Als gevolg van de gegeven axioma's voor een groep, kunnen enkele eenvoudige eigenschappen bewezen worden. We vatten deze in de volgende stelling samen en we laten het bewijs als oefening.

Stelling 8.1.1. *Zij $(G, \cdot)$ een groep.*

(1) *De vergelijking $xa = b$ (resp. $ax = b$) met onbekende x heeft juist één oplossing voor elke a en b, nl. $x = ba^{-1}$ (resp. $x = a^{-1}b$).*

(2) *De linkse en de rechtse schrappingswetten gelden, d.w.z. uit $ac = ad$ (resp. $ca = da$) volgt $c = d$.*

(3) *Er is slechts één enkel neutraal element e, en elk element $a \in G$ heeft juist één invers element a^{-1}.*

Bewijs als oefening. □

8.2 Ringen

Groepen vormen de juiste wiskundige basis om verzamelingen voorzien van één bewerking te beschrijven. Wanneer we echter terugkeren naar de vertrouwde bewerkingen van optelling en vermenigvuldiging van de gehele getallen, waarvan we de eigenschappen eerder hebben beschreven, dan moeten we vaststellen dat het concept van een groep niet voldoende is om deze bewerkingen volledig te beschrijven; in het bijzonder hebben we nog geen formeel kader gecreëerd dat iets zegt over de interactie tussen deze twee bewerkingen (optelling en vermenigvuldiging). Zo geldt bijvoorbeeld ook nog de distributiviteit van de vermenigvuldiging ten opzichte van de optelling. Daarom wordt het begrip *ring* ingevoerd.

8.2.1 Definities

We vertrekken van een geordend drietal (R, f, g), waarbij R een verzameling is en waarbij f en g binaire bewerkingen op R zijn. Voor de eenvoud zullen we voor f de additieve notatie $+$ gebruiken, terwijl we voor g de multiplicatieve notatie zullen gebruiken. Er is geen bezwaar dat gedacht wordt aan de optelling en de vermenigvuldiging van de gehele getallen of van de restklassen modulo m van de gehele getallen. Er zijn echter een heel groot aantal andere voorbeelden.

Het geordend drietal $(R, +, \cdot)$ wordt een *ring* genoemd dan en slechts dan als aan de volgende axioma's voldaan wordt:

(i) $(R, +)$ is een abelse groep met neutraal element 0;

(ii) Voor alle $a, b, c \in R$ geldt $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associatieve wet voor de vermenigvuldiging);

(iii) Er bestaat een element $e \in R \setminus \{0\}$ zodat voor alle $a \in R$ geldt: $e \cdot a = a \cdot e = a$ (e is het neutraal element voor de vermenigvuldiging);

(iv) Voor alle $a, b, c \in R$ geldt:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c\,.$$

Men zegt dat de vermenigvuldiging *distributief* is t.o.v. de optelling.

Opmerkingen

1. Men kan gemakkelijk bewijzen dat het neutraal element van een ring uniek bepaald is (oefening). Soms zullen we dit neutraal element ook

gewoon voorstellen door 1.

2. Als $(R, +, \cdot)$ een ring is zodanig dat voor alle $a, b \in R$ geldt dat $a \cdot b = b \cdot a$, dan zegt men dat $(R, +, \cdot)$ een *commutatieve* ring is.

3. De orde van een ring $(R, +, \cdot)$ is per definitie de orde van de onderliggende verzameling R.

4. Uit de definitie van een ring kan men niet besluiten dat de linkse of rechtse schrappingswet geldt. Het is ook mogelijk dat in een ring, elementen a en b bestaan die verschillend zijn van 0, maar waarvoor hun product 0 is. Dergelijke elementen worden daarom *nuldelers* van de ring genoemd.

5. Naar analogie met de groepen kan nu de definitie gegeven worden van een *ringmorfisme*, van *deelringen*, ... Aangezien we dit in het vervolg niet expliciet zullen gebruiken, laten we deze definities achterwege.

Voorbeelden

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ en $(\mathbb{Z}, +, \cdot)$ zijn (commutatieve) ringen voor de gewone optelling en vermenigvuldiging en bezitten geen nuldelers.

2. $(\mathbb{Z}/m, \oplus, \otimes)$ is de ring der gehele getallen modulo m, waarbij de optelling en vermenigvuldiging gedefinieerd worden modulo m, zoals in hoofdstuk 7 ingevoerd werd. Deze ring is een voorbeeld van een eindige commutatieve ring van de orde m. Indien m geen priemgetal is, dan bezit deze ring nuldelers. Zo is bijvoorbeeld $[3]_6 \otimes [2]_6 = [0]_6$. De schrappingswet geldt niet, want $[3]_6 \otimes [5]_6 = [3]_6 \otimes [1]_6$, maar nochtans is $[1]_6 \neq [5]_6$. Ondertussen weten wij dat dit een gevolg is van het feit dat in $\mathbb{Z}/6$ het element $[3]_6$ geen invers element bezit.

3. $(M_n(\mathbb{R}), +, \cdot)$ is de ring van de $n \times n$ matrices over de reële getallen voor de matrixoptelling en de matrixvermenigvuldiging. Deze ring is geen commutatieve ring. Ook hier geldt niet zomaar de linkse of rechtse schrappingswet en zijn de singuliere matrices (m.a.w. de matrices waarvan de determinant gelijk is aan 0) de nuldelers van de ring (zie cursus lineaire algebra).

8.2.2 Inverteerbare elementen van een ring

Definities

In paragraaf 7.3 hebben we de definitie van inverteerbare elementen in $\mathbb{Z}/m$ besproken. Deze definitie kan nu uitgebreid worden voor een willekeurige ring. Een element x van een ring R wordt *inverteerbaar* genoemd dan en slechts dan als x een invers element bezit voor de vermenigvuldiging. Met andere woorden, dan en slechts dan als er een element u in R bestaat waarvoor

$$u \cdot x = x \cdot u = 1.$$

Uit de definitie van een ring volgt nu onmiddellijk dat indien x inverteerbaar is, het element u uniek bepaald is; we kunnen daarom het symbool x^{-1} gebruiken i.p.v. u. Het is uiteraard onmiddellijk duidelijk dat indien x inverteerbaar is, het invers element x^{-1} eveneens inverteerbaar is. We stellen de deelverzameling van R die de inverteerbare elementen bevat voor door $R^\times$. Merk op dat voor de ring $\mathbb{Z}$ de verzameling $\mathbb{Z}^\times = \{1, -1\}$, terwijl bijvoorbeeld $(\mathbb{Z}/8)^\times = \{1, 3, 5, 7\}$.

Stelling 8.2.1. *De verzameling $R^\times$ van de inverteerbare elementen van een ring R vormen een groep voor de (restrictie van de) vermenigvuldiging.*

Bewijs. Veronderstel dat x en y inverteerbaar zijn en noem x^{-1} en y^{-1} hun respectieve inversen. Dan geldt

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= 1\\ (y^{-1}x^{-1})(xy) &= 1\,.\end{aligned}$$

Bijgevolg is $(xy)^{-1} = y^{-1}x^{-1}$ het invers element van xy. De verzameling $R^\times$ is dus gesloten voor de vermenigvuldiging. Aangezien uit de definitie van $R^\times$ volgt dat voor elk element x van $R^\times$ het invers element x^{-1} eveneens tot $R^\times$ behoort, volgt hieruit dat $R^\times$ een groep is voor de vermenigvuldiging. □

8.3 Lichamen en velden

Definitie

Een *lichaam* $\mathbb{F}$ is een ring waarvoor $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$. Bijgevolg is $\mathbb{F} \setminus \{0\}$ een groep voor de vermenigvuldiging. Indien de vermenigvuldiging bovendien commutatief is, dan wordt $\mathbb{F}$ een *veld* genoemd.

Voorbeelden

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ en $(\mathbb{C}, +, \cdot)$ zijn velden.

2. Uit Stelling 7.3.1 volgt dat $\mathbb{Z}/p$ een veld is dan en slechts dan als p een priemgetal is.

3. Noem i, j, k symbolen die aan de volgende vergelijkingen voldoen.

$$\begin{aligned} i^2 = \quad j^2 &= k^2 = -1 \\ ij = -ji &= k \\ jk = -kj &= i \\ ki = -ik &= j\,. \end{aligned}$$

   Dan is de verzameling $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ een oneindig lichaam dat geen veld is. Dit lichaam wordt het lichaam van de *quaternionen* genoemd.

   Het is overigens eenvoudig na te rekenen dat de optelling en vermenigvuldiging van twee willekeurige quaternionen er als volgt uit ziet.

$$\begin{aligned} &(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) \\ &\qquad = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k\,, \end{aligned}$$

$$\begin{aligned} &(a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) \\ &\quad = (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i \\ &\quad + (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)k\,. \end{aligned}$$

4. Alhoewel er heel wat voorbeelden bestaan van oneindige lichamen die geen velden zijn, is het vrij verrassend te moeten vaststellen dat elk lichaam met een eindig aantal elementen noodzakelijk een veld is. Dit werd voor het eerst bewezen door Wedderburn in 1905. We hebben reeds voorbeelden gezien van velden met een eindig aantal elementen, ook *eindige velden* genoemd, namelijk de velden $(\mathbb{Z}/p, +, \cdot)$ met p een priemgetal. Men kan zich nu afvragen of er nog andere eindige velden bestaan. Het antwoord werd gegeven door Evarist Galois. Het aantal elementen q van een eindig veld is noodzakelijk van de gedaante $q = p^h$, met p een priemgetal en h een natuurlijk getal verschillend van 0. Bovendien bestaat er voor elke $q = p^h$ op isomorfisme na juist één veld van die orde q; dit veld wordt genoteerd als $\mathbb{F}_q$. Als in het bijzonder $h = 1$, dan is $q = p$ een priemgetal, en is het veld $\mathbb{F}_p$ niets anders dan het veld $(\mathbb{Z}/p, +, \cdot)$.

5. De niet-singuliere $n \times n$ matrices met elementen in een veld $\mathbb{F}$ vormen een groep voor de vermenigvuldiging van matrices. Merk echter op dat deze matrices geen groep vormen voor de optelling, want de som van twee niet-singuliere $n \times n$ matrices is niet noodzakelijk niet-singulier.

8.4 Veeltermringen

8.4.1 Definitie

Een *veelterm* of *polynoom* over een ring R is elke uitdrukking van de gedaante

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n.$$

Hierbij noemt men x een *onbepaalde variabele* en noemt men de elementen $a_i, i \in \mathbb{N}[0, n]$, de *coëfficiënten* van de veelterm. Indien $a_n \neq 0$, dan noemen we n de graad van de veelterm. Er is geen reden om zeer expliciet te zijn over de variabele x zelf; veeltermen worden daarom zelfs soms voorgesteld als een geordende eindige rij

$$(a_0, a_1, a_2, \ldots, a_n).$$

Er bestaat met andere woorden een bijectie van de verzameling van veeltermen van de graad hoogstens n over een ring R op de verzameling R^{n+1}. De verzameling van al de veeltermen met coëfficiënten in de ring R wordt voorgesteld door $R[x]$. De veeltermen van de vorm (a_0) worden *constante veeltermen* genoemd en kunnen geïdentificeerd worden met de elementen van R. De *nulveelterm* is per definitie de constante veelterm (0). In het vervolg zullen we de constante veeltermen (a_0) kortweg als a_0 noteren.

Opmerking

In het vervolg zullen wij soms de veeltermen noteren in dalende volgorde van de exponenten van x:

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

De coëfficiënt van $a_n(\neq 0)$ wordt de *leidende coëfficiënt* genoemd. Indien $a_n = 1$, dan noemen we de veelterm een *monische veelterm*. Merk op dat indien we de verkorte (rij)notatie gebruiken, we steeds de coëfficiënten in stijgende volgorde van de exponenten zullen schrijven.

Veronderstel dat

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{en} \quad b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

twee veeltermen zijn over R met respectieve graad n en m. We zullen deze veeltermen verkort noteren door $a(x)$, respectievelijk $b(x)$. Zonder de algemeenheid te schaden, mogen wij veronderstellen dat $n \geq m$. Indien $n > m$, dan stellen we $b_{m+1} = b_{m+2} = \cdots = b_n = 0$. We kunnen nu de *som* $a(x)+b(x)$ en het *product* $a(x)b(x)$ van de veeltermen als volgt definiëren.

$$\begin{aligned} a(x) + b(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n, \\ a(x)b(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 \\ &\qquad + \cdots + a_nb_mx^{n+m}. \end{aligned}$$

Met andere woorden, de veelterm $s(x) = a(x) + b(x)$ is de veelterm gegeven door de rij $(s_0, s_1, \ldots, s_n)$ met

$$s_i = a_i + b_i \quad (0 \leq i \leq n),$$

terwijl $p(x) = a(x)b(x)$ de veelterm $(p_0, p_1, \ldots, p_{n+m})$ is met

$$p_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 \quad (0 \leq i \leq n + m),$$

waarbij we $a_k = 0$ stellen voor alle $k > n$ en $b_k = 0$ voor alle $k > m$. De optelling en de vermenigvuldiging van elementen in $R[x]$ worden dus gedefinieerd aan de hand van de optelling en vermenigvuldiging in R. We hebben daarom bewust geen andere notatie ingevoerd voor de optelling en de vermenigvuldiging in $R[x]$. Uit de definitie van een ring volgt dat indien de coëfficiënten van $a(x)$ en van $b(x)$ tot een ring R behoren, de coëfficiënten van hun som en hun product eveneens tot deze ring R behoren. Men kan eenvoudig (maar vrij omslachtig) bewijzen dat $R[x]$ voor de gedefinieerde optelling en vermenigvuldiging een commutatieve ring is, op voorwaarde dat R zelf een commutatieve ring is.

Merk echter op dat de graad van de som $a(x) + b(x)$ van twee veeltermen $a(x)$ en $b(x)$ strikt kleiner kan zijn dan de graad van $a(x)$ en van $b(x)$. Zo zal bijvoorbeeld in $(\mathbb{Z}/3)[x]$ de som van de veeltermen $x^2 + x + 1$ en $2x^2 + x + 1$ die beide van graad 2 zijn, gelijk zijn aan de veelterm $2x + 2$ van graad 1. Bovendien kan de graad van het product van twee veeltermen $a(x)$ en $b(x)$ strikt kleiner zijn dan de som van de graden van $a(x)$ en $b(x)$. Zo zal bijvoorbeeld in $\mathbb{Z}/6[x]$ het product van de veelterm $2x^2 + x + 4$ van graad 2 en de veelterm $3x + 1$ van graad 1 gelijk zijn aan de veelterm $5x^2 + x + 4$ van graad 2, want in $\mathbb{Z}/6$ is $3 \cdot 2 = 0$. Algemeen zal de graad van het product van twee veeltermen $a(x)$ en $b(x)$ kleiner zijn dan de som van de graden van deze veeltermen als de leidende coëfficiënten van $a(x)$ en $b(x)$ nuldelers van de ring zijn en als het product van deze leidende coëfficiënten gelijk is aan 0.

Opmerking

Een ring die nauw verwant is aan de veeltermring, is de ring van formele machtreeksen over een ring R, die we hebben ingevoerd[1] in sectie 4.1, en die we noteren als $R[[x]]$. De verificatie van de axioma's van een ring verloopt geheel analoog als bij de veeltermring $R[x]$.

8.4.2 Het delingsalgoritme voor veeltermen

Vanaf nu veronderstellen we dat de veeltermcoëfficiënten elementen zijn van een veld $\mathbb{F}$. Dit betekent echter hoegenaamd niet dat de ring $\mathbb{F}[x]$ een veld zal zijn (waarom?). Naar analogie met de ring van de gehele getallen bestaat ook voor de veeltermring $\mathbb{F}[x]$ een stelling over deelbaarheid van veeltermen.

Stelling 8.4.1. *Veronderstel dat $\mathbb{F}$ een veld is en dat $a(x)$ en $b(x)$ veeltermen zijn in $\mathbb{F}[x]$ waarbij $b(x) \neq 0$. Dan bestaan er unieke veeltermen $q(x)$ en $r(x)$ in $\mathbb{F}[x]$ zodanig dat*

$$a(x) = b(x)q(x) + r(x),$$

waarbij de graad van $r(x)$ kleiner is dan de graad van $b(x)$ of waarbij $r(x)$ de nulveelterm is.

Bewijs. We zullen inductie toepassen op de graad van de veelterm $a(x)$. Indien de graad van $a(x)$ kleiner is dan de graad van $b(x)$, dan is aan de stelling voldaan door $q(x)$ gelijk te stellen aan de nulveelterm en $r(x) = a(x)$ te nemen. We veronderstellen nu dat de graad van $b(x)$ gelijk is aan m en dat de graad van $a(x)$ gelijk is aan $n = m + k$ met $k \in \mathbb{N}$.

Stel

$$a(x) = a_{m+k}x^{m+k} + \cdots + a_0, \quad \text{en} \quad b(x) = b_m x^m + \cdots + b_0,$$

met $a_{m+k} \neq 0$, $b_m \neq 0$. Als inductiehypothese veronderstellen we dat de stelling waar is voor elke veelterm waarvan de graad kleiner is dan n.

Stel

$$\bar{a}(x) = a(x) - a_{m+k}b_m^{-1}x^k b(x).$$

De coëfficiënt van x^{m+k} in $\bar{a}(x)$ is

$$a_{m+k} - (a_{m+k}b_m^{-1})b_m = 0.$$

[1] In sectie 4.1 hebben we enkel de ring $\mathbb{R}[[x]]$ van formele machtreeksen over $\mathbb{R}$ ingevoerd, maar het is duidelijk hoe dit veralgemeend kan worden naar een willekeurige basisring R in plaats van $\mathbb{R}$.

Bijgevolg is de graad van $\bar{a}(x)$ kleiner dan de graad van $a(x)$. Wegens de inductiehypothese weten we dat er veeltermen $\bar{q}(x)$ en $r(x)$ bestaan zodanig dat

$$\bar{a}(x) = b(x)\bar{q}(x) + r(x),$$

waarbij $r(x)$ ofwel de nulveelterm is of waarbij de graad van $r(x)$ kleiner is dan de graad van $b(x)$. We stellen nu

$$q(x) = \bar{q}(x) + a_{m+k}b_m^{-1}x^k.$$

Dan volgt hieruit dat

$$a(x) = b(x)q(x) + r(x),$$

waarbij $r(x)$ aan de gestelde voorwaarden voldoet.

We moeten nu nog enkel bewijzen dat $q(x)$ en $r(x)$ uniek bepaald zijn. Veronderstel dat

$$a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x),$$

met $r_i(x)$ $(i = 1, 2)$ ofwel de nulveelterm ofwel is de graad van $r_i(x)$ $(i = 1, 2)$ kleiner dan de graad van $b(x)$. Dan geldt

$$b(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

De veelterm in het linkerlid is ofwel de nulveelterm (en dan is $q_1(x) = q_2(x)$) ofwel is de graad ten minste gelijk aan de graad van $b(x)$ (merk op dat we veeltermen over een veld $\mathbb{F}$ beschouwen). Anderzijds is de veelterm in het rechterlid ofwel de nulveelterm (en dan is $r_1(x) = r_2(x)$) ofwel is de graad ervan strikt kleiner dan de graad van $b(x)$. Bijgevolg moeten de veeltermen in beide leden de nulveelterm zijn en zal dus $q_1(x) = q_2(x)$ en $r_1(x) = r_2(x)$. □

8.4.3 Het algoritme van Euclides voor veeltermen

Naar analogie met de gehele getallen kunnen we nu ook definities geven en stellingen bewijzen over deelbaarheid van veeltermen. We noemen $g(x)$ een *deler* of *factor* van een veelterm $f(x)$ in $\mathbb{F}[x]$ als er een veelterm $h(x)$ bestaat in $\mathbb{F}[x]$ zodanig dat

$$f(x) = g(x)h(x).$$

Voor elke twee veeltermen $a(x)$ en $b(x)$ in $\mathbb{F}[x]$ noemen we $d(x)$ een *grootste gemene deler* van $a(x)$ en $b(x)$, notatie $\gcd(a(x), b(x))$, als

(i) $d(x)$ een deler is van $a(x)$ en van $b(x)$,

(ii) elke deler van $a(x)$ en van $b(x)$ eveneens deler is van $d(x)$.

Merk op dat uit de definitie niet volgt dat $d(x)$ uniek bepaald is. Indien inderdaad $d_1(x)$ en $d_2(x)$ beide grootste gemene delers zijn van $a(x)$ en $b(x)$, dan geldt $d_1(x) = \alpha d_2(x)$ met α een constante (veelterm). Het woord *grootste* in de term grootste gemene deler slaat echter op het feit dat de graad van $d(x)$ uniek bepaald is. Onder de verzameling van de grootste gemene delers bevindt zich dus steeds een (unieke) monische veelterm.

Om nu de $\gcd((a(x), b(x))$ in $\mathbb{F}[x]$ te berekenen herhalen we het argument zoals voor de gehele getallen, hetgeen nu aanleiding geeft tot het *algoritme van Euclides voor veeltermen over* $\mathbb{F}$. We kunnen dus de volgende opeenvolgende delingen uitvoeren.

$$\begin{aligned} b(x) &= a(x)q_1(x) + r_2(x) \\ a(x) &= r_2(x)q_2(x) + r_3(x) \\ r_2(x) &= r_3(x)q_3(x) + r_4(x) \\ &\vdots \\ r_{k-2}(x) &= r_{k-1}(x)q_{k-1}(x) + r_k(x) \\ r_{k-1}(x) &= r_k(x)q_k(x)\,. \end{aligned}$$

Uit de laatste vergelijking volgt dat $r_k(x)$ een deler is van $r_{k-1}(x)$. Indien we de vergelijkingen in omgekeerde volgorde doorlopen, dan volgt hieruit dat $r_k(x)$ een deler is van $r_{k-3}(x)$ enz., zodat $r_k(x)$ eveneens deler is van $a(x)$ en van $b(x)$. Door de achtereenvolgende substituties uit te voeren, kunnen we dus $r_k(x)$ schrijven in de vorm

$$\lambda(x)a(x) + \mu(x)b(x),$$

waarbij $\lambda(x)$ en $\mu(x)$ veeltermen zijn in $\mathbb{F}[x]$. Op die manier hebben we een analogon voor de Stelling 6.2.1 opgesteld.

Stelling 8.4.2. *Veronderstel dat* $\mathbb{F}$ *een veld is, en zij* $d(x)$ *een grootste gemene deler van de veeltermen* $a(x)$ *en* $b(x)$ *in* $\mathbb{F}[x]$. *Dan bestaan er veeltermen* $\lambda(x)$ *en* $\mu(x)$ *in* $\mathbb{F}[x]$ *zodanig dat*

$$d(x) = \lambda(x)a(x) + \mu(x)b(x).$$

Voorbeeld

Zoek een grootste gemene deler $d(x)$ *van*

$$a(x) = x^3 + 2x^2 + x + 1 \quad \textit{en} \quad b(x) = x^2 + 5$$

in $(\mathbb{Z}/7)[x]$ *en schrijf* $d(x)$ *in de vorm* $d(x) = \lambda(x)a(x) + \mu(x)b(x)$.

Oplossing
We moeten dus de deling van de polynomen $a(x)$ en $b(x)$ uitvoeren. Dit gebeurt op dezelfde manier als we gewoon zijn voor de veeltermen over bijvoorbeeld de reële getallen, alleen moeten we nu de coëfficiënten als elementen van $\mathbb{Z}/7$ beschouwen. We bekomen

$$x^3 + 2x^2 + x + 1 = (x^2 + 5)(x + 2) + (3x + 5).$$

Als volgende stap moeten we de deling van $x^2 + 5$ door $3x + 5$ uitvoeren. Merk op dat in $(\mathbb{Z}/7)[x]$ geldt dat $x^2 + 5 = 15x^2 + 5$. Hieruit volgt dat

$$x^2 + 5 = (3x + 5)(5x + 1).$$

Bijgevolg is $3x + 5$ een grootste gemene deler van de gegeven veeltermen. Aangezien we maar weinig delingen hebben uitgevoerd om $d(x)$ te bepalen, zijn de veeltermen $\lambda(x)$ en $\mu(x)$ vrij vlug te bepalen. We bekomen

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

Bijgevolg is $\lambda(x) = 1$ en $\mu(x) = 6x + 5$.

8.4.4 Ontbinden in factoren

In hoofdstuk 4 hebben we bewezen dat elk geheel getal op een unieke manier te ontbinden is in een product van priemgetallen. Aangezien we tot hiertoe de theorie van de veeltermen over een veld volledig naar analogie met de theorie van de gehele getallen hebben opgebouwd, kunnen we ons de vraag stellen of er ook een analogon voor priemgetallen bestaat.

Merk eerst en vooral op dat een constante veelterm verschillend van de nulveelterm altijd een deler is van een willekeurige veelterm $f(x)$ in $\mathbb{F}[x]$. Dergelijke triviale ontbinding of factorisatie zullen we in het vervolg uitsluiten. Een veelterm $f(x)$ in $\mathbb{F}[x]$ wordt *irreducibel* genoemd dan en slechts dan als $f(x)$ geen constante veelterm is en als $f(x) = g(x)h(x)$ in $\mathbb{F}[x]$ impliceert dat ofwel $g(x)$ ofwel $h(x)$ constante veeltermen zijn. Deze irreducibele veeltermen van $\mathbb{F}[x]$ zullen nu de rol overnemen van de priemgetallen in $\mathbb{Z}$. Er geldt dan ook de volgende stelling, waarvan we echter het (eenvoudig) bewijs achterwege laten.

Stelling 8.4.3. *Indien $f(x)$ een veelterm is in $\mathbb{F}[x]$ die geen constante veelterm is, dan kan $f(x)$ geschreven worden als een product van irreducibele veeltermen. Indien*

$$f(x) = g_1(x)g_2(x)\cdots g_r(x) = h_1(x)h_2(x)\cdots h_s(x),$$

dan is $r = s$ en bovendien bestaat er voor elke $g_i(x)$ $(i = 1, \ldots, r)$ juist één $h_j(x)$ $(j = 1, \ldots, r)$ zodanig dat $g_i(x) = \alpha_j h_j(x)$ met $\alpha_j \in \mathbb{F}^\times$.

Deze stelling zegt echter niet hoe we nu de ontbinding of factorisatie moeten vinden. Dit is in het algemeen een zeer moeilijk probleem. Nochtans bestaat er wel een vrij eenvoudig algoritme om na te gaan of een veelterm een lineaire factor, i.e. een factor van de vorm $g(x) = a_1 x + a_0$ $(a_1 \neq 0)$, bezit. Aangezien $a_1 \neq 0$ kunnen we de lineaire veelterm steeds in de vorm $x - \alpha$ brengen. Indien $f(x) = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$, dan zal voor elke $\alpha \in \mathbb{F}$ gelden dat $f(\alpha) = f_n \alpha^n + f_{n-1} \alpha^{n-1} + \cdots + f_0$ een element is van $\mathbb{F}$. Nu geldt de volgende zogenaamde *factorisatiestelling*.

Stelling 8.4.4. *Veronderstel dat $\mathbb{F}$ een veld is en veronderstel dat $f(x)$ een veelterm is in $\mathbb{F}[x]$. Dan is $x - \alpha$ dan en slechts dan een factor van $f(x)$ in $\mathbb{F}[x]$ als $f(\alpha) = 0$ in $\mathbb{F}$.*

Bewijs. Veronderstel dat $x - \alpha$ een deler is van $f(x)$, dan is

$$f(x) = (x - \alpha) g(x).$$

Hieruit volgt echter dat

$$f(\alpha) = (x - \alpha) g(\alpha) = 0 \cdot g(\alpha) = 0.$$

Omgekeerd, veronderstel dat $f(\alpha) = 0$ in $\mathbb{F}$. Dan bestaan er veeltermen $q(x)$ en $r(x)$ in $\mathbb{F}[x]$ zodanig dat

$$f(x) = (x - \alpha) q(x) + r(x),$$

waarbij $r(x)$ een constante veelterm moet zijn. Aangezien echter

$$0 = f(\alpha) = (\alpha - \alpha) q(\alpha) + r(\alpha) = r(\alpha),$$

volgt hieruit dat $r(x)$ de nulveelterm is. Bijgevolg is $x - \alpha$ een deler van $f(x)$. □

Voor elke veelterm $f(x)$ van $\mathbb{F}[x]$ worden de elementen α van $\mathbb{F}$ waarvoor geldt dat $f(\alpha) = 0$, de *wortels* genoemd van de vergelijking $f(x) = 0$.

Stelling 8.4.5. *Indien $\mathbb{F}$ een veld is en indien $f(x)$ een veelterm is van de graad n $(n \geq 1)$ in $\mathbb{F}[x]$, dan bezit de vergelijking $f(x) = 0$ ten hoogste n wortels in $\mathbb{F}$.*

Bewijs. Veronderstel dat de vergelijking m wortels $\alpha_1, \alpha_2, \ldots, \alpha_m$ bezit. Dan zal wegens de factorisatiestelling

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m)g(x),$$

voor een zekere $g(x)$ in $\mathbb{F}[x]$. Aangezien de coëfficiënten tot een veld behoren, zal de graad van het product in het rechterlid de som van de graden van de factoren zijn. Hieruit volgt dat de graad van $f(x)$ ten minste m is, of gelijkwaardig hiermee dat het aantal wortels van $f(x) = 0$ ten hoogste n is. □

Zoals het bij de gehele getallen niet steeds eenvoudig is om een gegeven getal in priemfactoren te ontbinden, is het hier niet steeds eenvoudig om een gegeven veelterm te ontbinden in irreducibele factoren. Om de eventuele lineaire factoren van een veelterm $f(x)$ in $\mathbb{F}[x]$ te vinden, weten we dat we gewoon $f(\alpha)$ moeten uitrekenen waarbij α het veld $\mathbb{F}$ zal doorlopen. Indien dit veld een eindig aantal elementen bezit, dan hebben we op die manier een bruikbaar algoritme. Misschien heeft de veelterm $f(x)$ geen lineaire factoren, in dit geval hebben we dus al de berekeningen voor niets gedaan. Niemand zegt echter dat er eventueel geen factoren van hogere graad kunnen optreden. In sommige gevallen bestaan er efficiënte algoritmen voor het zoeken van irreducibele factoren van een gegeven veelterm. De studie van deze algoritmen valt echter buiten het raam van deze cursus. We beperken ons hier tot een voorbeeld dat echter niet als een voorbeeld van een efficiënt algoritme mag beschouwd worden.

Voorbeeld

Zoek de irreducibele factoren van $x^4 + 1$ *in* $(\mathbb{Z}/3)[x]$.

Oplossing.
We zoeken eerst de eventuele lineaire factoren. Stel $x^4 + 1 = f(x)$, dan is

$$f(0) = 1 \quad \text{en} \quad f(1) = f(2) = 2.$$

Er zijn bijgevolg geen lineaire factoren. Indien de veelterm dus reducibel is, dan moet hij noodzakelijk het product zijn van twee irreducibele kwadratische veeltermen. Bijgevolg geldt dan

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

voor zekere $a, b, c, d \in \mathbb{Z}/3$. Aangezien

$$(x^2+ax+b)(x^2+cx+d)$$
$$= x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd\,,$$

moeten a, b, c, d oplossingen zijn van het volgende stelsel over $\mathbb{Z}/3$:

$$\begin{cases} a+c=0 \\ b+d+ac=0 \\ ad+bc=0 \\ bd=1\,. \end{cases}$$

Men vindt eenvoudig de volgende oplossingen: $a=1$ en $b=c=d=2$, of $c=1$ en $a=b=d=2$ (oefening). Beide oplossingen leiden tot dezelfde ontbinding in $(\mathbb{Z}/3)[x]$, namelijk

$$x^4+1=(x^2+x+2)(x^2+2x+2)\,.$$

Opmerking

Alhoewel het zoeken naar een irreducibele veelterm in $\mathbb{F}[x]$ dus niet steeds eenvoudig is, kan men bewijzen dat in $(\mathbb{Z}/p)[x]$ (p een priemgetal) steeds een irreducibele veelterm te vinden is voor elke graad n. Deze veeltermen zullen de bouwstenen vormen voor de constructie van de eindige velden.

Oefeningen

1. Ontbind x^8-1 in $(\mathbb{Z}/3)[x]$.
2. Ontbind x^3+5x^2+5 in $(\mathbb{Z}/11)[x]$.
3. Zoek alle monische polynomen in $(\mathbb{Z}/3)[x]$ die irreducibel zijn.
4. Bewijs dat x^2+2x+2 irreducibel is in $(\mathbb{Z}/3)[x]$.