Hoofdstuk 3

Equivalentierelaties

▷ SCHAUM §2.8: Equivalence Relations

Twee belangrijke voorbeelden van equivalentierelaties in de informatica: resten (modulo rekenen) en cardinaliteit (aftelbaarheid).

3.1 Modulo Rekenen

▷ SCHAUM §11.8: Congruence Relation, ook §3.4 (Modular Arithmetic).

We leggen een constante $m \geq 2$ vast, en definieren een relatie op $\mathbb{Z}$: equivalentie modulo m. Getallen met dezelfde rest na deling door m beschouwen we voortaan als gelijk.

3.1 Definitie. Voor $x, y \in \mathbb{Z}$, geldt dat x equivalent is aan y (modulo m), genoteerd als $x \equiv y \bmod m$, wanneer $x - y$ deelbaar is door m. □

3.2 Lemma. *De relatie $x \equiv y \bmod m$ is een equivalentierelatie.* □

> Bewijs. *reflexief.* $x - x = 0$ is deelbaar door m, dus $x \equiv x \bmod m$.
> *symmetrisch.* Als $x \equiv y \bmod m$ dan is $x - y$ deelbaar door m. Dan is ook $y - x = -(x - y)$ deelbaar door m, dus $y \equiv x \bmod m$.
> *transitief.* Als $x \equiv y \bmod m$ en Als $y \equiv z \bmod m$ dan zijn $x - y$ en $y - z$ deelbaar door m. Dan is ook $(x - y) + (y - z) = (x - z)$ deelbaar door m, dus $x \equiv z \bmod m$. □

De equivalentieklassen van deze relatie bestaan uit getallen met dezelfde rest bij deling door m. Ze worden wel *restklassen* genoemd. Er zijn verschillende manieren in omloop om de klassen van de modulo-equivalentie aan te geven: $[x]_m$ zoals algemeen voor equivalentierelaties, of $x \bmod m$, of simpelweg $\overline{x}$. Modulo m zijn

er m verschillende restklassen: $[0]_m$, $[1]_m$, $\ldots [m-1]_m$. Dus $0,1,\ldots,m-1$ is een complete verzameling representanten, uit elke klasse precies één element.

De restklassen modulo 7 zijn bijvoorbeeld:
$[0]_7 = \{\ldots -14,-7,0,7,14,21,\ldots\}$
$[1]_7 = \{\ldots -13,-6,1,8,15,22,\ldots\}$
$[2]_7 = \{\ldots -12,-5,2,9,16,23,\ldots\}$
$[3]_7 = \{\ldots -11,-4,3,10,17,24,\ldots\}$
$[4]_7 = \{\ldots -10,-3,4,11,18,25,\ldots\}$
$[5]_7 = \{\ldots -9,-2,5,12,19,26,\ldots\}$
$[6]_7 = \{\ldots -8,-1,6,13,20,27,\ldots\}$

Rekenen met resten. Zij $m \geq 2$. Geef de restklasse $[r]_m$ aan met $\overline{r}$. We definiëren de optelling, aftrekking en vermenigvuldiging van twee restklassen als volgt: $\overline{r}+\overline{s} = \overline{r+s}$, $\overline{r}-\overline{s} = \overline{r-s}$, en $\overline{r}\cdot\overline{s} = \overline{rs}$. De restklassen met deze operaties vormen de algebraische structuur die genoteerd wordt met $\mathbb{Z}_m$.

Deze bewerkingen zijn goed gedefinieerd, dat wil zeggen dat hun uitkomsten eenduidig vastliggen, en dus niet afhangen van de getallen r en s die toevallig uit de restklasse gekozen zijn. Zijn r' en s' getallen met $r' \equiv r \bmod m$ en $s' \equiv s \bmod m$; dan geldt ook $\overline{r} = \overline{r'}$ en $\overline{s} = \overline{s'}$. Nu geven de bovenstaande definities enerzijds

$$\overline{r}+\overline{s} = \overline{r+s}, \quad \overline{r}-\overline{s} = \overline{r-s}, \quad \overline{r}\cdot\overline{s} = \overline{r}\cdot\overline{s} = \overline{rs}.$$

en anderzijds

$$\overline{r}+\overline{s} = \overline{r'}+\overline{s'} = \overline{r'+s'}, \quad \overline{r}-\overline{s} = \overline{r'}-\overline{s'} = \overline{r'-s'}, \quad \overline{r}\cdot\overline{s} = \overline{r'}\cdot\overline{s'} = \overline{r's'}.$$

Dus opdat de uitkomsten van $\overline{r}+\overline{s}$, $\overline{r}-\overline{s}$, $\overline{r}\cdot\overline{s}$ eenduidig vastliggen moet gelden dat $\overline{r'+s'} = \overline{r+s}$, $\overline{r'-s'} = \overline{r-s}$, en $\overline{r's'} = \overline{rs}$. Maar aan dit laatste wordt wegens Theorem 11.22 inderdaad voldaan. (▷ SCHAUM p.275.)

Ter illustratie geven we de opteltabel en vermenigvuldigingstabel van $\mathbb{Z}_5$ en $\mathbb{Z}_6$. Let op een opvallend verschil: bij $\mathbb{Z}_5$ bestaat voor ieder element $\overline{x}$ een element $\overline{y}$ zodat $\overline{xy} = \overline{1}$ (de inverse). Dat kenmerkende verschil wordt veroorzaakt door het feit dat 5 een priemgetal is. Omdat 2 een deler is van 6, heeft 2 geen inverse (modulo 6).

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

We noemen zonder bewijs een stel rekenregels voor de optelling en vermenigvuldiging van restklassen modulo m die erg veel lijken op de regels van optelling en vermenigvuldiging van gehele getallen.

3.3 Stelling. *Geef de restklasse $[x]_m$ aan met $\overline{x}$.*
Dan geldt voor alle $\overline{a}$, $\overline{b}$, $\overline{c}$ in $\mathbb{Z}_m$:
(i) $\overline{a}+\overline{b}=\overline{b}+\overline{a}$, $\overline{a}\cdot\overline{b}=\overline{b}\cdot\overline{a}$ (commutatieve regels)*;*
(ii) $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$, $(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{a}\cdot(\overline{b}\cdot\overline{c})$ (associatieve regels)*;*
(iii) $\overline{a}\cdot(\overline{b}+\overline{c})=\overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$ (distributieve regel)*;*
(iv) $\overline{a}+\overline{0}=\overline{a}$ ($\overline{0}$ neutraal element van optelling)*;*
(v) $\overline{a}\cdot\overline{1}=\overline{a}$ ($\overline{1}$ neutraal element van vermenigvuldiging)*;*
(vi) *er is een unieke restklasse $\overline{x}$ met $\overline{a}+\overline{x}=\overline{0}$, namelijk $\overline{x}=\overline{-a}$* (tegengestelde). □

Let op dat niet alle eigenschappen van de operaties op gehele getallen overgenomen kunnen worden. Op $\mathbb{Z}$ geldt: *als $xy=0$ dan $x=0$ of $y=0$*. Uit de vermenigvuldigingstabel voor $\mathbb{Z}_6$ blijkt bijvoorbeeld dat $\overline{3}\cdot\overline{4}=\overline{0}$.

We geven enkele toepassingen, die het begrip modulo rekenen motiveren.

3.4 Voorbeeld.

1. 1 januari 2000 valt op zaterdag. Op welke dag valt 13 mei 2023?

> Nummer de dagen. We geven 1 januari 2000 nummer 1, 2 januari 2000 nummer 2 en nummeren van daaraf door. Dus 31 januari 2000 heeft nummer 31, 1 februari 2000 nummer 32 ,..., 31 december 2000 nummer 366, 1 januari 2001 nummer 367, enzovoort. De dagen met nummers 1,8,15,..., dat wil zeggen de dagen met nummers in de restklasse $[1]_7$ vallen op zaterdag, de dagen met nummers in $[2]_7$ op zondag, ..., de dagen met nummers in $[6]_7$ op donderdag en tenslotte de dagen met nummers in $[0]_7$ op vrijdag. We moeten dus de restklasse modulo 7 bepalen van het nummer van 13 mei 2023.
> Geef de restklasse $[a]_7$ aan met $\overline{a}$.
>
> Het nummer van 13 mei 2023 is

$23 \cdot 365$	(23 jaar)
$+6$	(6 schrikkeldagen)
$+31+28+31+30+13$	(aantal dagen in 2023 tot en met 13 mei)

De restklasse modulo 7 hiervan is (omdat $\overline{23} = \overline{2}$, $\overline{365} = \overline{1}$, enz.)

$\overline{23} \cdot \overline{365} + \overline{6} + \overline{31} + \overline{28} + \overline{31} + \overline{30} + \overline{13}$
$= \overline{2} \cdot \overline{1} + \overline{6} + \overline{3} + \overline{0} + \overline{3} + \overline{2} + \overline{6}$ (tel de getallen op)
$= \overline{22} = \overline{1}$.

Dus 13 mei 2023 valt op zaterdag.

2. Zij $s(m)$ de som van de cijfers (in het tientallig stelsel) van een getal m. Dan is $m \equiv s(m) \pmod 9$.

Namelijk zij $c_k c_{k-1} \cdots c_1 c_0$ de representatie van m in het tientallig stelsel. Dan is $m = c_0 + c_1 \cdot 10 + c_2 \cdot 10^2 + \cdots + c_k \cdot 10^k$. Als we met $\overline{a}$ de restklasse $[a]_9$ aangeven dan is $\overline{10} = \overline{1}$. Dus $\overline{m} = \overline{c_0} + \overline{c_1} \cdot \overline{1} + \overline{c_2} \cdot \overline{1}^2 + \cdots + \overline{c_k} \cdot \overline{1}^k = \overline{c_0} + \overline{c_1} + \cdots + \overline{c_k} = \overline{c_0 + c_1 + \cdots + c_k} = \overline{s(m)}$

3. Bewijs dat $x^2 - 1$ deelbaar is door 8 voor elk oneven getal x.

We moeten natuurlijk werken met restklassen modulo 8. Schrijf een restklasse $[x]_8$ als $\overline{x}$. Er geldt:

$x^2 - 1$ is deelbaar door $8 \iff x^2 \equiv 1 \pmod 8 \iff \overline{x^2} = \overline{1} \iff \overline{x}^2 = \overline{1}$.

Wanneer x oneven is, dan is de rest van x bij deling door 8 gelijk aan $1, 3, 5$ of 7, met andere woorden $\overline{x}$ is een van de restklassen $\overline{1}, \overline{3}, \overline{5}, \overline{7}$. Dus we moeten nagaan of $\overline{x}^2 = \overline{1}$ voor $\overline{x} = \overline{1}, \overline{3}, \overline{5}, \overline{7}$. Maar dit volgt direct uit het volgende rijtje:

$\overline{1}^2 = \overline{1}$, $\overline{3}^2 = \overline{9} = \overline{1}$, $\overline{5}^2 = \overline{25} = \overline{1}$, en $\overline{7}^2 = \overline{49} = \overline{1}$.

4. $5^n - 2^n$ is een drievoud voor alle $n \in \mathbb{N}$.

We werken modulo 3, en moeten laten zien dat $5^n \equiv 2^n \pmod 3$ voor alle $n \in \mathbb{N}$. Dat geldt omdat $5 \equiv 2 \pmod 3$. (Ik denk dat nu geen verdere inductie nodig is.)

Zonder restklassen bewijst men deze gelijkheid wel eens met inductie, via $5^{n+1} - 2^{n+1} = 5 \cdot (5^n - 2^n) + 3 \cdot 2^n$. Nu zijn hierin de factoren $5^n - 2^n$ (inductieveronderstelling) en 3 deelbaar door drie, en daarmee de hele som.

5. Bereken 103785163 mod 17.

We lossen het probleem cijfer-voor-cijfer op, dat wil zeggen we berekenen de resten voor achtereenvolgens 1, 10, 103, 1037, ...

Hierbij ontstaat elk getal door het vorige met tien te vermenigvuldigen en het passende cijfer op te tellen. De berekening van de resten volgt dit recept.

1, $10 + \mathbf{0} \equiv 10$, $100 + \mathbf{3} \equiv 1$, $10 + \mathbf{7} \equiv 0$, $0 + \mathbf{8} \equiv 8$, $80 + \mathbf{5} \equiv 0$, $0 + \mathbf{7} \equiv 7$, $70 + \mathbf{1} \equiv 3$, $30 + \mathbf{6} \equiv 2$, $20 + \mathbf{3} \equiv 6$.

Hiermee is het antwoord $103785163 \equiv 6 \bmod 17$ bereikt.

3.2 Aftelbaarheid

▷ SCHAUM 3.7 Cardinality

Tellen. Een verzameling A heeft n elementen als we deze elementen kunnen paren aan de getallen $1,2,...,n$; dwz. er is een bijectie $f : \{1,2,...,n\} \to A$. De eis van surjectiviteit zorgt ervoor dat elk element geteld wordt, de eis van injectiviteit dat geen elementen dubbel worden geteld.

Tussen twee (eindige) verzamelingen bestaat een bijectie precies dan als ze evenveel elementen hebben. Tenminste dat is intuitief zo, en wordt hier formeel gemaakt.

3.5 Definitie. Verzamelingen A en B heten *gelijkmachtig* als er een bijectie tussen A en B bestaat. We schrijven dan $A \simeq B$. □

3.6 Stelling. *Voor eindige verzamelingen A en B geldt: A en B zijn gelijkmachtig desdals* $|A| = |B|$.

> Bewijs. Stel A heeft n elementen en A en B zijn gelijkmachtig. Er zijn dus bijecties $f : \{1,...,n\} \to A$ en $g : A \to B$. De samenstelling $g \circ f$ is een bijectie $\{1,...,n\} \to B$ en toont aan dat B ook n elementen heeft.
>
> Stel A en B hebben beide n elementen. Er zijn dus bijecties $f : \{1,...,n\} \to A$ en $h : \{1,...,n\} \to B$. De bijectie $h \circ f^{-1} : A \to B$ toont aan dat A en B gelijkmachtig zijn. □

Voor oneindige verzamelingen is er een vreemde, tegenintuitieve, situatie: een verzameling kan gelijkmachtig zijn met een echte deelverzameling. Heeft die deelverzameling dan evenveel elementen als de gehele verzameling?

3.7 Voorbeeld. $\mathbb{R}$ en $\mathbb{R}^+$ zijn gelijkmachtig, $\mathbb{R}$ en het open interval $\langle 0,1\rangle$ zijn gelijkmachtig.

Laat E de verzameling even natuurlijke getallen zijn. Dan geldt $E \subset \mathbb{N}$ (echt) maar tegelijkertijd zijn $\mathbb{N}$ en E gelijkmachtig vanwege de bijectie $f : \mathbb{N} \to E$ met $f(i) = 2 \cdot i$ voor $i \in \mathbb{N}$.

Eindige verzamelingen kunnen kennelijk alleen gelijkmachtig zijn als ze evenveel elementen bezitten. Maar hoe zit dat met oneindige verzamelingen? We weten dat $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, maar bestaan er bijecties tussen elk van deze verzamelingen?

3.8 Opmerking. Gelijkmachtigheid is een relatie tussen verzamelingen met bijzondere eigenschappen. Voor alle verzamelingen A, B en C geldt:

reflexief: $A \simeq A$.
symmetrisch: als $A \simeq B$, dan is $B \simeq A$.
transitief: als $A \simeq B$ en $B \simeq C$, dan is $A \simeq C$.

Een relatie met deze drie eigenschappen heet een *equivalentierelatie*, zie ▷ SCHAUM§ 2.8. □

3.9 Definitie. Een verzameling A heet *aftelbaar* als A eindig is, of als $\mathbb{N}$ gelijkmachtig is met A. In het laatste geval heet A *oneindig* aftelbaar. □

Als $\mathbb{N}$ gelijkmachtig is met verzameling A dan is er een bijectie $f : \mathbb{N} \to A$. De elementen $f(0), f(1), f(2), \ldots$ vormen precies een *opsomming* (of *aftelling*) van A; elk element van A komt precies één keer in de rij voor.

We hebben gezien dat E, de verzameling van even natuurlijke getallen, aftelbaar is, terwijl E 'half zoveel' elementen bevat als $\mathbb{N}$. De verzameling $\mathbb{Z}$, 'dubbel zo groot' als $\mathbb{N}$, is ook aftelbaar.

3.10 Stelling. *$\mathbb{Z}$ is aftelbaar.*

> Bewijs. We kunnen $\mathbb{Z}$ 'aftellen' door om-en-om positieve en negatieve getallen te nemen: $0, 1, -1, 2, -2, 3, -3, \ldots$ Formeel krijgen we zo de bijectie $f : \mathbb{N} \to \mathbb{Z}$ gedefinieerd door $f(n) = \begin{cases} -\frac{n}{2} & \text{als } n \text{ even} \\ \frac{n-1}{2} & \text{als } n \text{ oneven} \end{cases}$ □

De bijectie $f : \mathbb{N} \to A$ bij een (oneindige!) aftelbare verzameling A somt de elementen van A allemaal op (surjectief) en zonder herhaling (injectief). Soms lijkt het praktischer om herhalingen toe te staan, vooral ook omdat we dan ook eindige verzamelingen mee laten doen. Dat is geen probleem.

3.11 Stelling. *A is een niet-lege verzameling. A is aftelbaar desdals er een surjectieve $f : \mathbb{N} \to A$ bestaat.*

> Bewijs. Als A oneindig aftelbaar is bestaat er een bijectie $f : \mathbb{N} :\to A$ volgens de definitie. Natuurlijk is f de gezochte surjectie. Als A eindig is kunnen we een surjectieve $g : \{1, \ldots, n\} \to A$ vinden, die we naar heel $\mathbb{N}$ als domein uitbreiden door bijvoorbeeld een element uit A te kiezen (A mag daarom niet leeg zijn) dat beeld wordt van de overige getallen.
>
> Nu omgekeerd. De 'surjectieve aftelling' $f(0), f(1), f(2), \ldots$ van A kan herhalingen bevatten, die we moeten verwijderen om een bijectie $g : \mathbb{N} \to A$ te krijgen. Kies dus $g(0) = f(0)$ en voor $n \geq 1, g(n) = f(i)$ waarbij i de kleinste index waarvoor $f(i) \notin \{g(0), g(1), \ldots, g(n-1)\}$.
>
> Voor eindige A stopt dit proces als alle elementen gevonden zijn. □

We passen deze stelling meteen toe. Als twee verzamelingen aftelbaar zijn, dan is ook hun vereniging dat.

3.12 Stelling. *Als A_1 en A_2 aftelbaar zijn, dan ook $A_1 \cup A_2$.*

Bewijs. Gegeven de aftelbaarheid van A_i bestaan er surjecties $f_i : \mathbb{N} \to A_i, i = 1,2$. De vereniging $A_1 \cup A_2$ wordt afgeteld door de twee afzonderlijke reeksen af te wisselen $f_1(0), f_2(0), f_1(1), f_2(1), \ldots$ Hier kunnen herhalingen in voorkomen: deze samenstelling is surjectief, niet noodzakelijk injectief. Formeler, laat $g : \mathbb{N} \to A_1 \cup A_2$ gedefinieerd zijn door $g(n) = \begin{cases} f_1(\frac{n}{2}) & \text{als } n \text{ even} \\ f_2(\frac{n-1}{2}) & \text{als } n \text{ oneven} \end{cases}$.
Nu is g surjectief, want A_1 is het beeld van de even getallen en A_2 van de oneven getallen. Tenslotte is $A_1 \cup A_2$ aftelbaar wegens voorafgaande stelling. □

In zekere zin is deze methode dezelfde als bij de aftelbaarheid van $\mathbb{Z}$. Het is duidelijk dat $\mathbb{N}$ aftelbaar is (toch?) maar ook $-\mathbb{N} = \{0, -1, -2, -3, ...\}$. dus ook $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$.

De voorafgaande stelling geldt ook bij aftelbaar oneindige verenigingen! ▷ SCHAUM Theorem 3.2

3.13 Stelling. *Als A_i aftelbaar is, voor alle $i \in \mathbb{N}$, dan ook $A = \bigcup_{i \in \mathbb{N}} A_i$.*

Bewijs. Gegeven de aftelbaarheid van A_i bestaan er surjecties $f_i : \mathbb{N} \to A_i, i \in \mathbb{N}$. Beschouw nu de elementen van de vereniging A als opgenomen in een twee-dimensionale, dubbeloneindige, matrix. De elementen van A_i staan in de i-de rij (we beginnen te tellen bij rij nul):

$$\begin{array}{ccccc} f_0(0) & f_0(1) & f_0(2) & f_0(3) & \ldots \\ f_1(0) & f_1(1) & f_1(2) & f_1(3) & \ldots \\ f_2(0) & f_2(1) & f_2(2) & \ldots & \\ f_3(0) & f_3(1) & f_3(2) & \ldots & \\ \vdots & \vdots & \vdots & \ddots & \end{array}$$

De elementen van A worden 'afgeteld' door een ingenieuze wandeling door de matrix, langs de opeenvolgende diagonalen:
$f_0(0), f_0(1), f_1(0), f_0(2), f_1(1), f_2(0), f_0(3), f_1(2), f_2(1), f_3(0), f_0(4), ...$
Hieruit is een surjectieve $g : \mathbb{N} \to A$ te construeren, maar de wandeling is intuitief duidelijker dan het precieze recept:
$g(\frac{n \cdot (n+1)}{2} + k) = f_k(n-k)$ voor $0 \leq k \leq n$.
De wandeling wordt wel een *Cantor-wandeling* genoemd. □

Hieruit volgt een onverwacht feit.

3.14 Stelling. $\mathbb{Q}$ *is aftelbaar.*

Bewijs. We laten zien dat $\mathbb{Q}^+$ aftelbaar is, hieruit volgt de aftelbaarheid van $\mathbb{Q}$ omdat dat zelf weer de vereniging is van aftelbare verzamelingen: $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$.

Kies voor elke $k \geq 1$ de verzameling $A_k = \{\frac{1}{k}, \frac{2}{k}, \frac{3}{k}, \ldots\}$ als alle (niet vereenvoudigde) positieve breuken met noemer k,

Duidelijk is A_k aftelbaar, en $\mathbb{Q}^+ = \bigcup_{k\geq 1} A_k$. Aftelbaarheid van $\mathbb{Q}^+$ volgt vanwege de aftelbare vereniging van aftelbare verzamelingen.

$$\begin{array}{cccc} \frac{0}{0} & \frac{0}{1} & \frac{0}{2} & \frac{0}{3} & \cdots \\ \frac{1}{0} & \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \cdots \\ \frac{2}{0} & \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \cdots \\ \frac{3}{0} & \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

De geschetste Cantor-wandeling levert een 'opsomming' van $\mathbb{Q}^+$ met vele herhalingen: $\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{4}{2}, \frac{3}{3}, \frac{2}{4}, \frac{1}{5}, \frac{6}{1}, \ldots$ □

Als $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ aftelbaar zijn, is dan ook $\mathbb{R}$ aftelbaar? Zijn alle oneindige verzamelingen aftelbaar? Nee. ▷ SCHAUM Theorem 3.3.

3.15 Stelling. $\mathbb{R}$ *is* niet *aftelbaar.* □

We geven geen bewijs. Het bewijs maakt gebruik van de oneindige decimale schrijfwijze van reele getallen, en van *diagonalisatie*, een principe dat terugkomt in het bewijs van de volgende stelling.

Voor een eindige verzameling A met n elementen bevat $\mathscr{P}(A)$ precies 2^n elementen. Omdat $\mathscr{P}(A)$ meer elementen bevat dan A zijn de verzamelingen A en $\mathscr{P}(A)$ niet gelijkmachtig. Dit geldt ook voor oneindige verzamelingen, maar moet op een andere manier bewezen worden. ▷ SCHAUM Theorem 3.4 (Cantor's theorem)

3.16 Stelling. *Laat A een verzameling zijn. A is* niet *gelijkmachtig met $\mathscr{P}(A)$.*

Bewijs. We laten dit zien door middel van tegenspraak. Neem aan dat A gelijkmachtig is met $\mathscr{P}(A)$, en we tonen aan dat hieruit een contradictie volgt. Vanwege de aanname is er een bijectie $f : A \to \mathscr{P}(A)$. Het beeld $f(a)$ van $a \in A$ is een deelverzameling van A, en we kunnen ons afvragen of $a \in f(a)$.

Kies de verzameling $V = \{a \in A \mid a \notin f(a)\}$. Omdat $V \subseteq A$ en omdat f surjectief is, is er een element $b \in A$ met $V = f(b)$. Voor willekeurige $a \in A$ geldt: $a \in V$ desdals $a \notin f(a)$. Voor b geldt dus ook: $b \in V$ desdals $b \notin f(b)$.

Omdat $V = f(b)$, vinden we een tegenspraak, dus b kan niet bestaan, en er is geen bijectie tussen A en $\mathscr{P}(A)$.

Het argument in dit bewijs staat bekend als *diagonalisatie*; deze terminologie wordt duidelijk als we het speciale geval $A = \mathbb{N}$ bekijken, zie overheads van het college. □

3.17 Gevolg. $\mathscr{P}(\mathbb{N})$ *is niet aftelbaar.* □

Slotwoord. Een ander gevolg is dat er oneindig veel typen oneindigheid ('cardinaalgetallen', dat zijn equivalentieklassen van de gelijkmachtigheidsrelatie $\simeq$) bestaan: $\mathbb{N}$, $\mathscr{P}(\mathbb{N})$, $\mathscr{P}(\mathscr{P}(\mathbb{N}))$, ... zijn alle paarsgewijs niet gelijkmachtig. Waar past hier $\mathbb{R}$? Er geldt dat $\mathbb{R}$ en $\mathscr{P}(\mathbb{N})$ gelijkmachtig zijn, maar een bewijs daarvan laten we hier achterwege.

De cardinaliteit van $\mathbb{N}$ wordt wel aangegeven als aleph-nul $\aleph_0$, de eerste oneindige cardinaliteit. De cardinaliteit van $\mathbb{R}$ is gelijk aan $2^{\aleph_0}$. Het is niet bekend of dit de kleinste vorm van oneindig is die na $\aleph_0$ komt: de gelijkheid $\aleph_1 = 2^{\aleph_0}$ heet wel de continuum hypothese.

Ook ▷ SCHAUM Theorem 3.5 (Schröder-Bernstein) vinden we te ingewikkeld om hier te behandelen. Die stelling zegt dat de relatie $\leq$ op cardinaalgetallen antisymmetrisch is.