Foundations of Computer Science

Fundamentele Informatica 1

Hendrik Jan Hoogeboom
Jeannette de Graaf

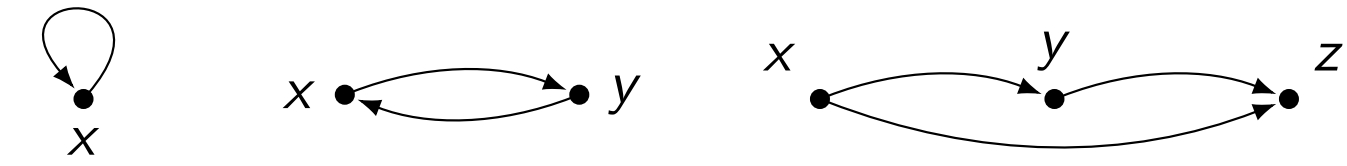
Bachelor Informatica (& specialisaties)
Universiteit Leiden

Najaar 2020

Universiteit
Leiden
Leiden Institute of
Advanced Computer Science

Hoofdstuk 8

Twee Equivalentierelaties



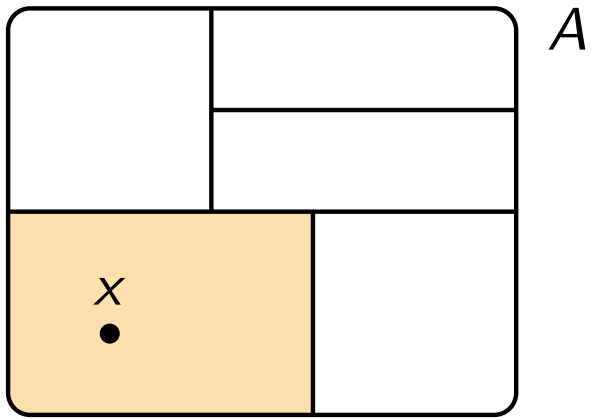
reflexief symmetrisch transitief

$R \subseteq A \times A$ *equivalentierelatie*

- *reflexief* $x\ R\ x$ voor alle $x \in A$
- *symmetrisch* uit $x\ R\ y$ volgt dat $y\ R\ x$ voor alle ...
- *transitief* uit $x\ R\ y$ en $y\ R\ z$ volgt dat $x\ R\ z$ voor alle ...
  als $x\ R^n\ z$ dan $x\ R\ z$ voor alle $n \geqslant 1$ voor alle ...

$R \subseteq A \times A$ equivalentierelatie

partitie van A



equivalentieklasse $[x] = \{ z \mid x \, R \, z \}$

1. rekenen met resten modulo
2. kardinaliteit aantal elementen aftelbaarheid

- in $\mathbb{Z}$ $\quad x \equiv y \pmod 5 \iff x - y$ deelbaar door 5

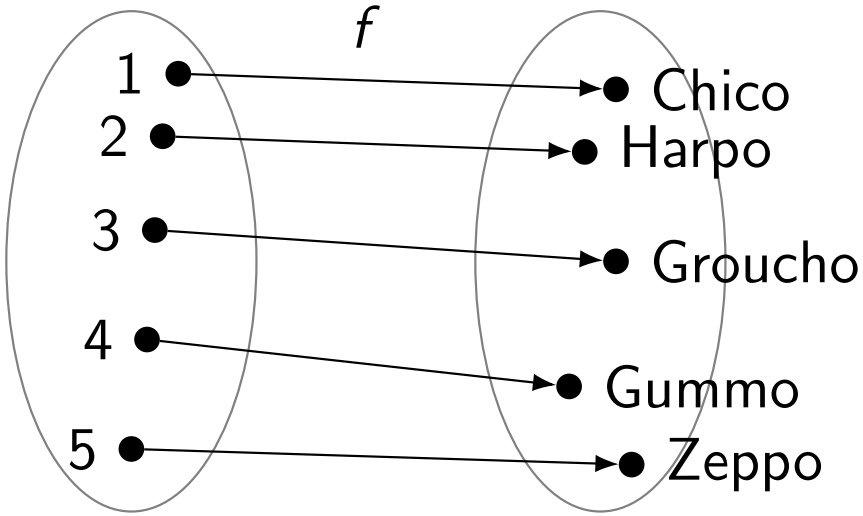
-11	-6	-1	4	9	14	19	$\cdots$
$\cdots$	-7	-2	3	8	13	18	$\cdots$
$\cdots$	-8	-3	2	7	12	17	$\cdots$
$\cdots$	-9	-4	1	6	11	16	$\cdots$
$\cdots$	-10	-5	0	5	10	15	$\cdots$

eigenschap: rest (bij deling door 5)

Sch 11.8 Congruence relation

V eindig $\quad |V| = n$

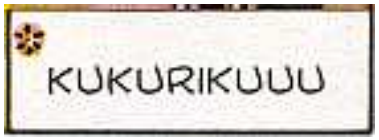
$f : \{1, 2, \ldots, n\} \to V \quad$ bijectie



gelijkmachtig *equipotent* $\quad A \simeq B \iff$ bijectie $f : A \to B$

Sch 3.7 Cardinality

8 Twee Equivalentierelaties
- Modulo rekenen
- Aftelbaarheid



17u.

8 uur later

1u.

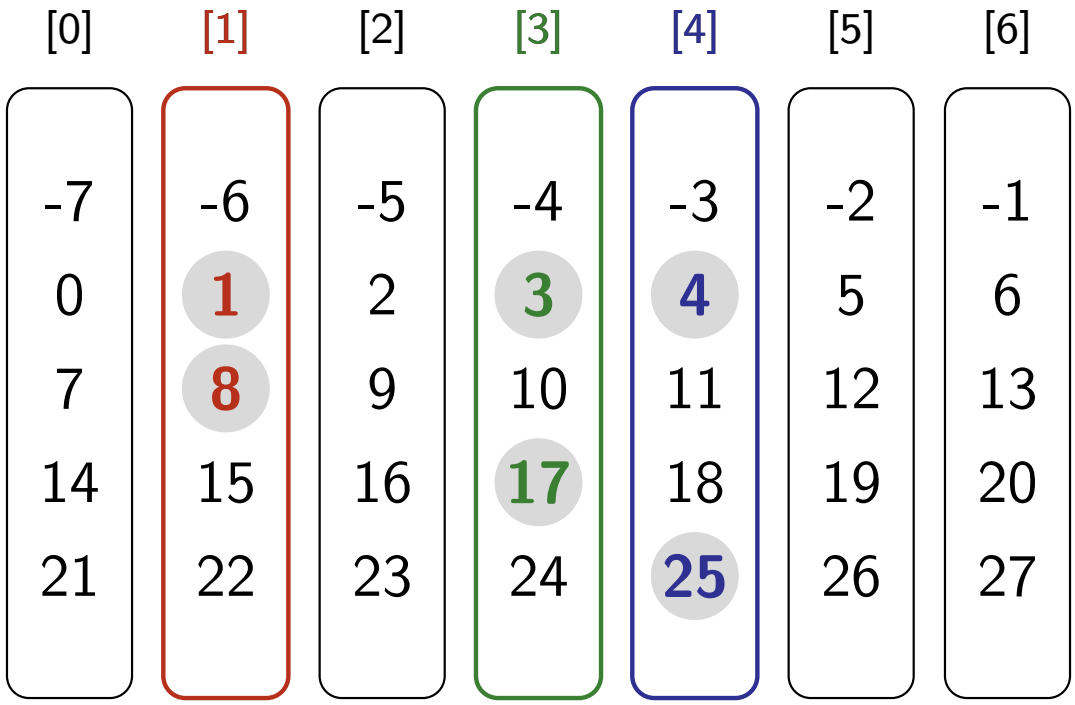
$17 + 8 \equiv 1 \pmod{24}$

rekenen modulo 24

```
// is jaar een schrikkeljaar?
bool schrikkel (int jaar) {
   return ( jaar % 4 == 0
            && ( jaar % 400 == 0 || jaar % 100 != 0 ) );
}//schrikkel
```

```
i = 0
while i < 100:
    if i % 10 == 0:
        print("This happens once every ten times!")
    i += 1
```

$x \equiv y \pmod 7$



$$1 + 3 = 4$$
$$8 + 17 = 25$$

$x \equiv y \pmod m \iff x - y$ deelbaar door m

gelijk/congruent modulo m ($m > 1$, geheel, vast gekozen)

Thm. 11.21, Prob. 11.34

$\equiv \pmod m$ is een equivalentierelatie

bewijs. (slordige modulo notatie)

reflexief $a \equiv a\ (m)$ voor alle a

$a - a = 0$ is deelbaar door m

symmetrisch als $a \equiv b\ (m)$ dan $b \equiv a\ (m)$ voor alle a, b

$b - a = -(a - b)$ is deelbaar door m

transitief als $a \equiv b\ (m)$ en $b \equiv c\ (m)$ dan $a \equiv c\ (m)$ voor ...

$a - c = (a - b) + (b - c)$ is deelbaar door m

$\mathbb{Z}$ gehele getallen
$m > 1$, vast

rest $x = q \cdot m + r \quad 0 \leqslant r < m$

- $x \equiv y \pmod{m}$
- $x - y$ deelbaar door m
- $x - y$ is een veelvoud van m
- x en y hebben dezelfde rest (bij deling door m)
- $\dfrac{x-y}{m}$ is geheel

`%` `div` `rem` `mod`

- $x \equiv 0 \pmod{m}$
- x deelbaar door m
- x is een veelvoud van m
- x heeft rest 0 (bij deling door m)
- $\dfrac{x}{m}$ is geheel

$\equiv \pmod m$ gedraagt zich netjes bij operaties $+$ en $*$

Thm. 11.22 tov. vaste m

als $a \equiv a' \ (m)$ en $b \equiv b' \ (m)$ dan

- $a + b \equiv a' + b' \ (m)$
- $a - b \equiv a' - b' \ (m)$
- $a \cdot b \equiv a' \cdot b' \ (m)$

voorbeeld $72 \equiv 2$ $143 \equiv 3$ modulo 7

$72 + 143 = 215$	$2 + 3 = 5$	$215 \equiv 5$
$72 - 143 = -71$	$2 - 3 = -1$	$-71 \equiv -1$
$72 \cdot 143 = 10296$	$2 \cdot 3 = 6$	$10296 \equiv 6$

bewijs. gegeven $a - a'$ en $b - b'$ deelbaar door m

$(a + b) - (a' + b') = (a - a') + (b - b')$ deelbaar door m

$(a - b) - (a' - b') = (a - a') - (b - b')$ deelbaar door m

$(a \cdot b) - (a' \cdot b') = a \cdot (b - b') + (a - a') \cdot b'$ deelbaar door m

$$a^{2k} = (a^k)^2$$
$$a^{2k+1} = a^{2k} \cdot a$$

$12^{43} \pmod{71}$

recursief

$43 = 42 + 1$	$12^{43} \equiv 25 \cdot 12 \equiv 300 \equiv 16$
$42 = 2 \cdot 21$	$12^{42} \equiv -5 \cdot -5 \equiv 25$
$21 = 20 + 1$	$12^{21} \equiv 30 \cdot 12 \equiv 360 \equiv -5$
$20 = 2 \cdot 10$	$12^{20} \equiv 32 \cdot 32 \equiv 1024 \equiv 30$
$10 = 2 \cdot 5$	$12^{10} \equiv 48 \cdot 48 \equiv 2304 \equiv 32$
$5 = 4 + 1$	$12^5 \equiv 4 \cdot 12 \equiv 48$
$4 = 2 \cdot 2$	$12^4 \equiv 2 \cdot 2 = 4$
$2 = 2 \cdot 1$	$12^2 \equiv 12 \cdot 12 = 144 \equiv 2$
	$12^1 \equiv 12$

bij berekeningen met optellen en vermenigvuldigen getallen door simpele equivalente waarde vervangen

laatste cijfer $\rightsquigarrow$ modulo 10

dag van de week $\rightsquigarrow$ modulo 7

deelbaar door m $\rightsquigarrow$ modulo m

vb. bepaal laatste cijfer van 3^{234}

laatste cijfer $\rightsquigarrow$ modulo 10 rekenen

machten van 3 (modulo 10)

3^0	3^1	3^2	3^3	$3^4 = 3^3 \cdot 3$
1	3	9	$27 \equiv 7$	$7 \cdot 3 = 21 \equiv 1$

$3^4 \equiv 1 \pmod{10}$

$$3^{234} = 3^{4 \cdot 58 + 2} = \underbrace{(3^4)^{58}}_{(3^4)\cdot\ldots\cdot(3^4)} \cdot 3^2 \equiv 1^{58} \cdot 9 \equiv 9$$

let op: de exponent is *niet* modulo 10 genomen!

x deelbaar door 9 als som van de cijfers van x deelbaar door 9

$232.029 = 25781 \cdot 9$
$2 + 3 + 2 + 0 + 2 + 9 = 18$

x deelbaar door 9 $\iff$ $x \equiv 0 \pmod 9$

$$10 \equiv 1 \pmod 9$$
$$10^2 \equiv 1^2 \equiv 1 \pmod 9$$
$$10^k \equiv 1^k \equiv 1 \pmod 9$$

$c_k \ldots c_2 c_1 c_0 =$
$c_k 10^k + \cdots + c_2 10^2 + c_1 10^1 + c_0 10^0 \equiv$
$c_k + \cdots + c_2 + c_1 + c_0 \pmod 9$

$$\sum_{i=0}^{k} c_i 10^i \equiv \sum_{i=0}^{k} c_i \pmod 9$$

$5^n - 2^n$ is een drievoud voor $n \geqslant 0$

$5^{n+1} - 2^{n+1} = 5 \cdot (5^n - 2^n) + 3 \cdot 2^n$ is een drievoud

drievoud $\rightsquigarrow$ modulo 3 rekenen

$5 \equiv 2 \pmod 3$

$5^n \equiv 2^n \pmod 3$ (voor alle n)

$5^n - 2^n \equiv 2^n - 2^n \equiv 0 \pmod 3$

op welke dag valt 13 mei 23 ? (1 jan 2000 zaterdag)

weekdag $\rightsquigarrow$ modulo 7 rekenen

za	zo	ma	di	wo	do	vr
1	2	3	4	5	6	0

jaar 365 dagen $365 \equiv 1 \pmod 7$

jan	feb	mrt	apr	mei	jun	jul	aug	sep	okt	nov	dec
31	28*	31	30	31	30	31	31	30	31	30	31
3	0*	3	2	3	2	3	3	2	3	2	3

*elke vier jaar schrikkeldag (ook in 2000...) tip: knokkels

23 jaar $\times$ 365 dagen/jaar
$+$ 6 schrikkeldagen 2000 tm 2022 $\lceil \frac{23}{4} \rceil$
$+$ jan tm apr $+$ 13 dagen in 2023

$23 \cdot 365 + 6 + 31 + 28 + 31 + 30 + 13 \equiv$
$2 \cdot 1 + 6 + 3 + 0 + 3 + 2 + 6 \equiv 22 \equiv 1$ zaterdag

$\mathbb{Z}_6 = \{0, 1, 2, \ldots, 5\}$

$4 + 5 = 3 + 6 \qquad 4 \cdot 5 = 2 + 18$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$*$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

let op: *nuldelers* $3 \cdot 4 = 0$

niet '$x \cdot y = 0$ dan $x = 0$ of $y = 0$'

$\mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\}$

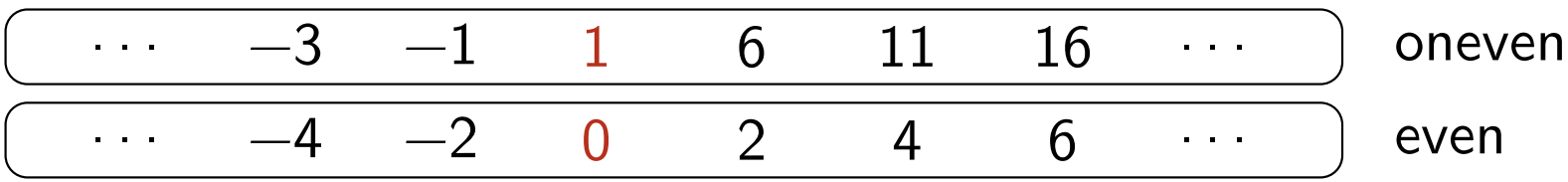
$4 + 5 = 2 + 7 \qquad 4 \cdot 5 = 6 + 14$

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

$*$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

x even $\quad x \equiv 0 \pmod 2 \quad \frac{x}{2}$ is geheel

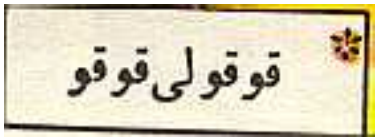
x oneven $\quad x \equiv 1 \pmod 2 \quad \frac{x-1}{2}$ is geheel



nul is even

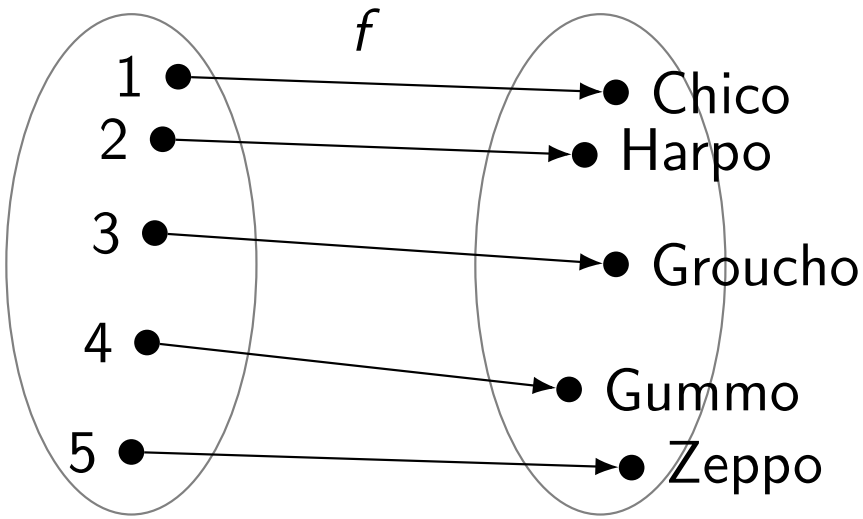
8 Twee Equivalentierelaties

- Modulo rekenen
- Aftelbaarheid



V eindig $\quad |V| = n$

$f : \{1, 2, \ldots, n\} \to V \quad$ bijectie



gelijkmachtig *equipotent* $\quad A \simeq B \iff$ bijectie $f : A \to B$

Sch 3.7 Cardinality

gelijkmachtig $A \simeq B \iff$ bijectie $f : A \to B$

'evenveel elementen als'

equivalentierelatie zie Functies

– reflexief $A \simeq A$

indentiteit $\mathrm{id} : A \to A$

– symmetrisch als $A \simeq B$ dan $B \simeq A$

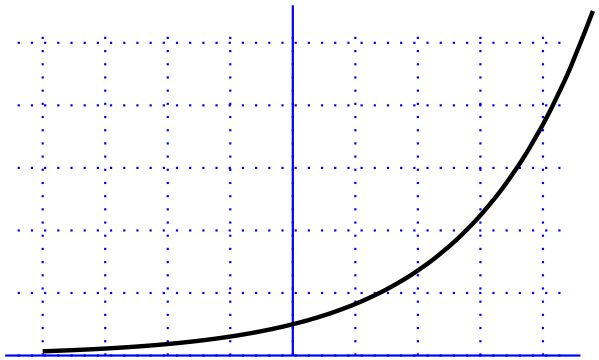
inverse $f : A \to B$ dan $f^{-1} : B \to A$

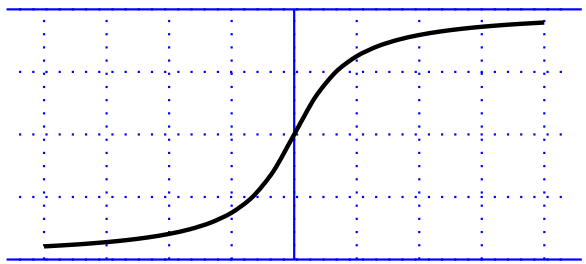
– transitief als $A \simeq B$ en $B \simeq C$ dan $A \simeq C$

compositie $f : A \to B$, $g : B \to C$ dan $g \circ f : A \to C$

gelijkmachtig $A \simeq B \iff$ bijectie $f : A \to B$

$\mathbb{R} \simeq \mathbb{R}^+$ $\mathbb{R} \simeq (0, 1)$





aftelling, opsomming

$\mathbb{N}:$	0	1	2	3	4	5	6	7	$\cdots$
$A:$	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	$\cdots$

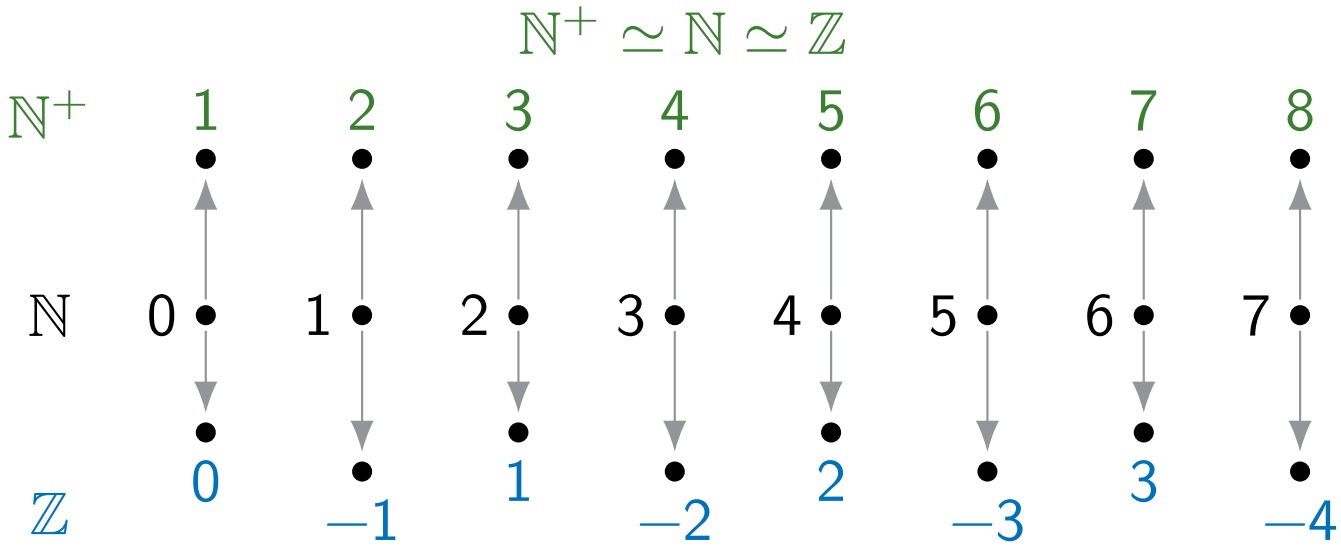
aftelbaar – eindig of
– $\mathbb{N} \simeq A$ bijectie tussen $\mathbb{N}$ en A

Prob. 3.11

$\mathbb{Z}$ is aftelbaar

$$f : \mathbb{N} \to \mathbb{Z} \qquad f(n) = \begin{cases} \frac{n}{2} & \text{als n even} \\ -\frac{n+1}{2} & \text{anders} \end{cases}$$

$\mathbb{N}:$	0	1	2	3	4	5	6	7	$\cdots$
$\mathbb{Z}:$	0	-1	1	-2	2	-3	3	-4	$\cdots$



the Open University: youtube

aftelbaar			overaftelbaar	
$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	
		$\mathbb{N} \times \mathbb{N}$	$\mathcal{P}(\mathbb{N})$	
		Cantor wandeling	diagonalisatie	

Thm. 3.3. $(0, 1)$ is overaftelbaar

$0.999\cdots = 1.000\cdots$

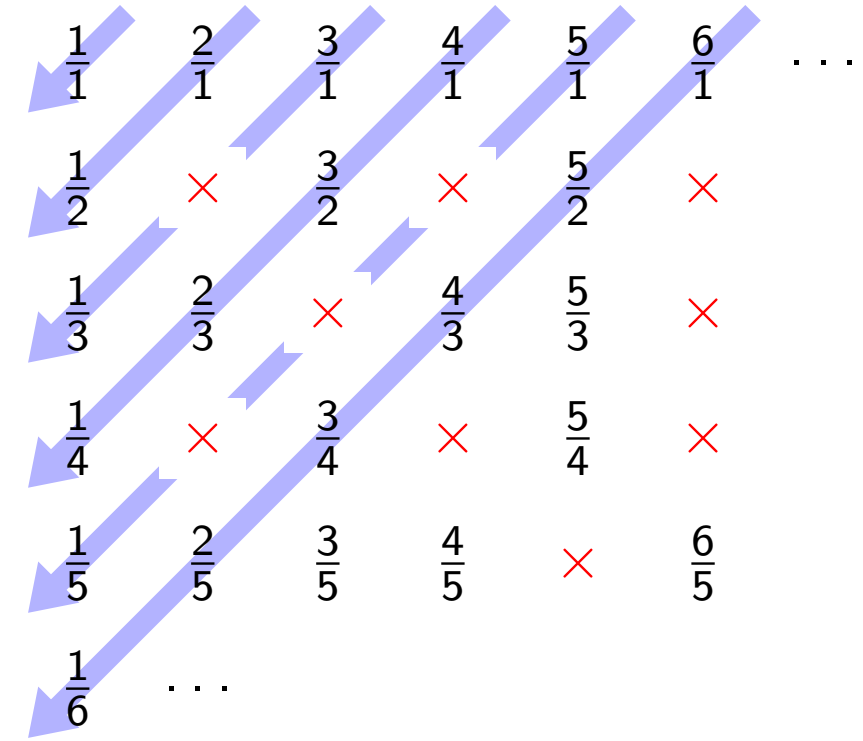
Cantor wandeling $\mathbb{Q}$ aftelbaar

Thm. 3.2. aftelbare vereniging van aftelbare verzamelingen is aftelbaar

diagonalisatie $\mathcal{P}(\mathbb{N})$ is niet aftelbaar

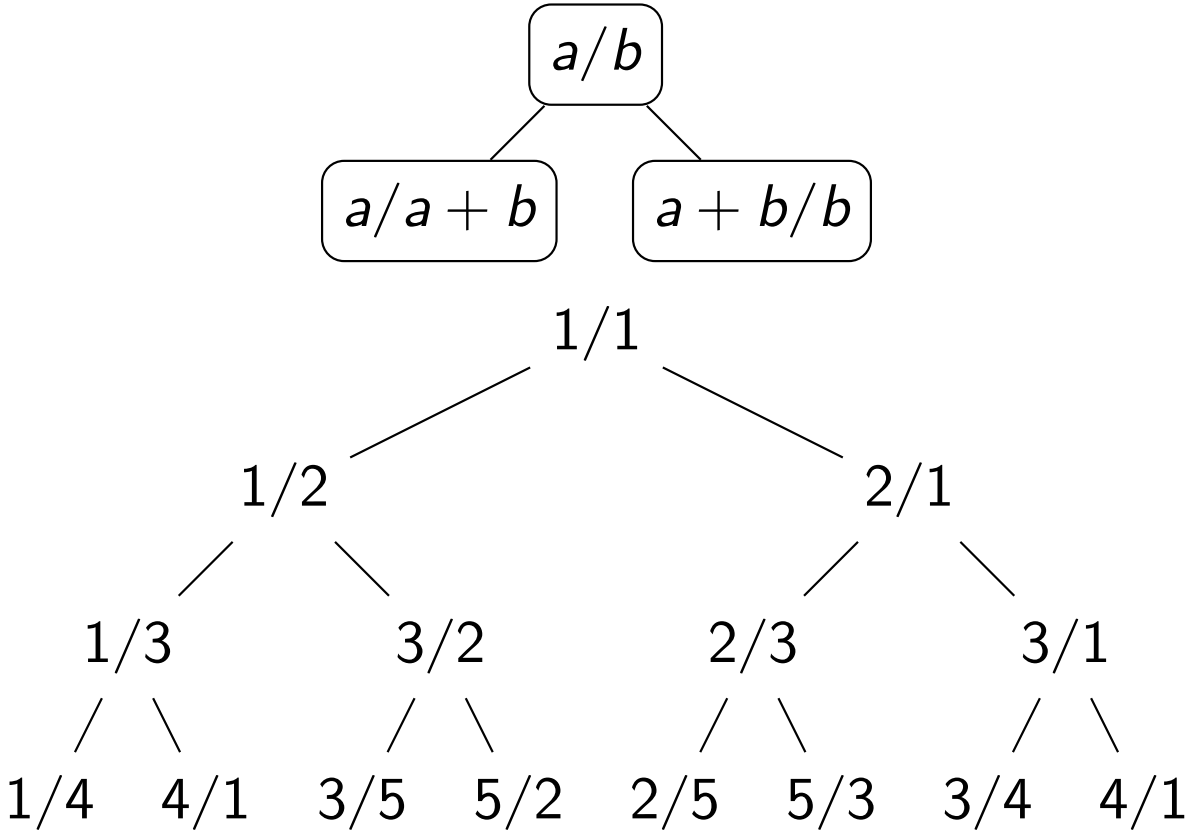
Thm. 3.4. A is niet gelijkmachtig met $\mathcal{P}(A)$

$\mathbb{Q}^+$ is aftelbaar



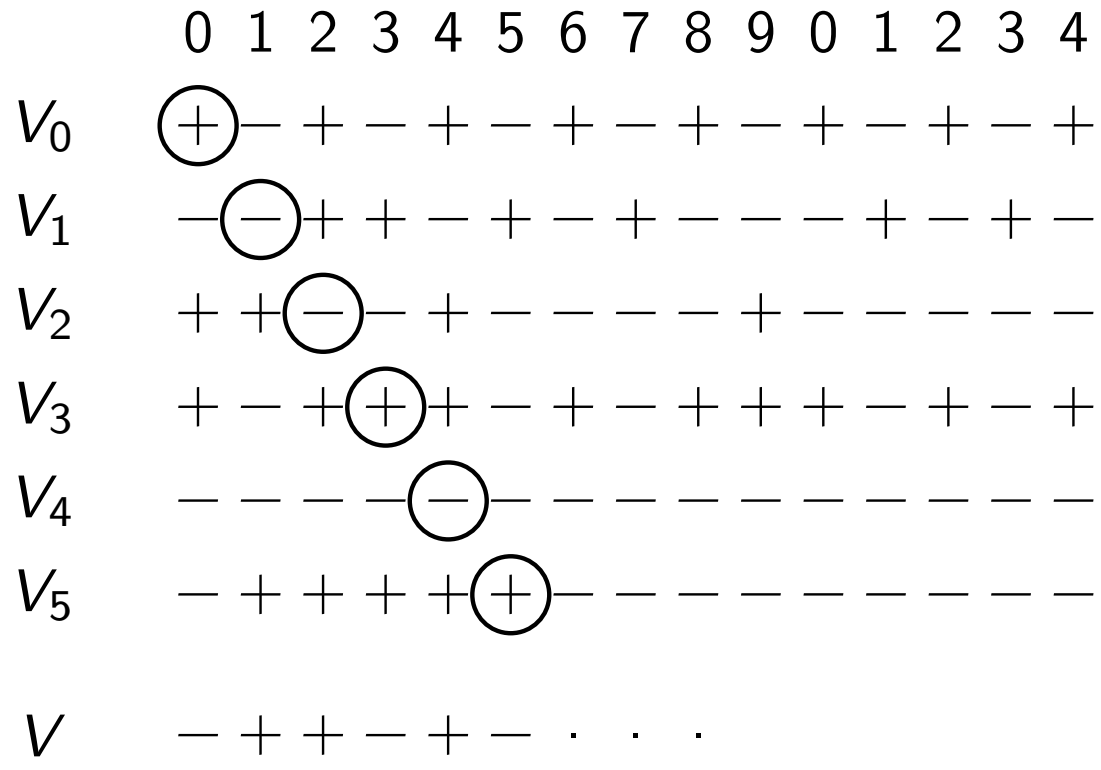
$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{1}{5}, \frac{6}{1}, \frac{5}{2}, \ldots$$

Calkin-Wilf breuken zonder herhaling



$\mathcal{P}(\mathbb{N})$ is *niet* aftelbaar

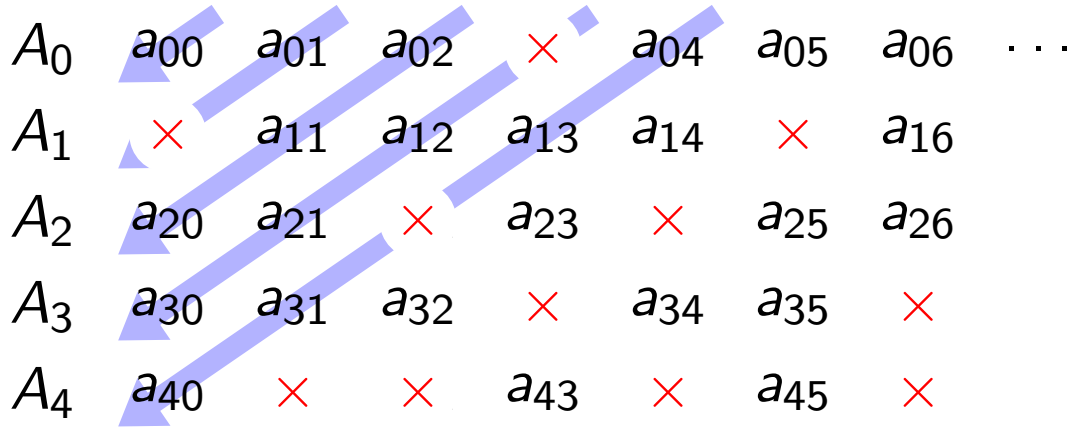
ongerijmde, stel wél $V_0, V_1, V_2, \ldots$ opsomming



$V = \{\, k \in \mathbb{N} \mid k \notin V_k \,\}$ maar $V \neq V_k$ (alle k)

A_k aftelbaar voor $k \in \mathbb{N}$

$\bigcup_{k\in\mathbb{N}} A_k$ is aftelbaar



$A_k = \{a_{kj} \mid j \in \mathbb{N}\}$ verzameling - horizontaal

$D_k = \{a_{ij} \mid i + j = k\}$ $k = 0, 1, 2, \ldots$ diagonalen

$B_n = D_n - \bigcup_{k<n} D_k$ $n = 0, 1, 2, \ldots$ nieuwe elementen

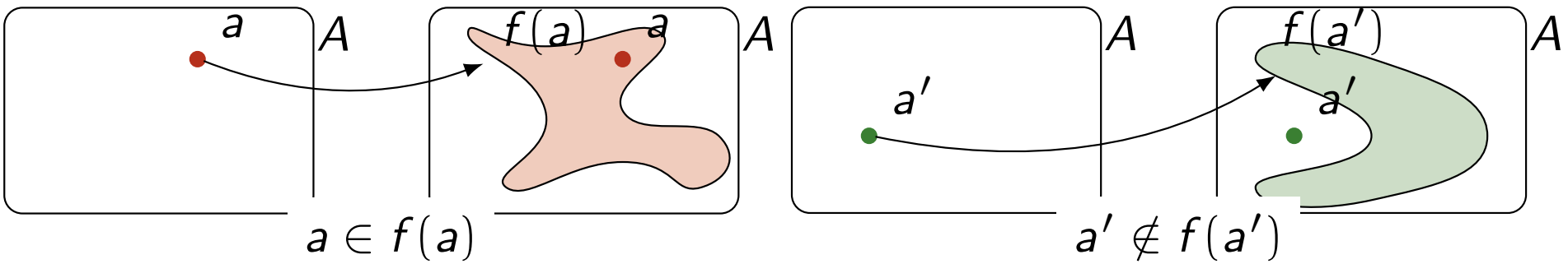
	$\lvert B_0\rvert$	$\lvert B_1\rvert$			$\lvert B_2\rvert$			$\lvert B_3\rvert$				$\lvert B_4\rvert$
0	1	2	3	4	5	6	7	8	9	10	11	12
a_{00}	a_{01}	a_{02}	a_{11}	a_{20}	a_{12}	a_{21}	a_{30}	a_{04}	a_{13}	a_{31}	a_{40}	a_{05}

Thm. 3.4, Prob. 3.25

voor elke verzameling A geldt $A \not\simeq \mathcal{P}(A)$

ongerijmde stel bijectie $f : A \to \mathcal{P}(A)$

$a \in A$ dan $f(a) \subseteq A$



definieer $B = \{\, x \in A \mid x \notin f(x) \,\}$

f surjectief: er is een b met $f(b) = B$

$$b \notin f(b) \underset{\substack{\text{definitie } B \\ x \notin f(x)}}{\iff} \boxed{b \in B} \underset{\substack{\text{keuze } b \\ B = f(b)}}{\iff} b \in f(b)$$

$|A| \leqslant |B|$ $\quad f : A \to B$ injectief

hoogstens evenveel

$|A| < |\mathcal{P}(A)|$

steeds grotere 'oneindigheden'

$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots$

$|A| = n$ A eindig

$|\mathbb{N}| = \aleph_0$ *aleph nul*

kleinste oneindige kardinaalgetal

$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}| = 2^{\aleph_0}$

$\aleph_1$ aleph één? eerste kardinaalgetal na $\aleph_0$

continuümhypothese $\aleph_1 = 2^{\aleph_0}$

$(0,1) \simeq (0,1)^2 = (0,1) \times (0,1)$

$0.b_1 b_2 b_3 b_4 \cdots \mapsto (0.b_1 b_3 \ldots, 0.b_2 b_4 \ldots)$

je le vois, mais je ne le crois pas

$|A| \leqslant |B|$ $f : A \to B$ injectief

hoogstens evenveel

☒Thm. 3.5 Schroeder-Bernstein

$|A| \leqslant |B|$ en $|B| \leqslant |A|$ dan $A \simeq B$

☞ er bestaat geen verzameling V van alle verzamelingen (!)

$$D = \{\, X \in V \mid X \notin X \,\} \quad \text{diagonalisatie}$$

$$D \in D \overset{\text{definitie}}{\Longleftrightarrow} D \notin D$$

END.