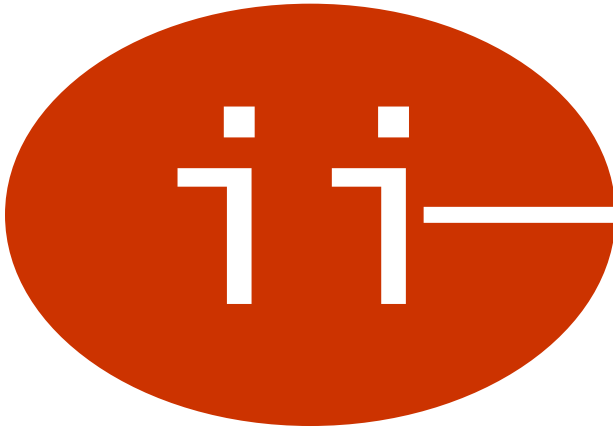
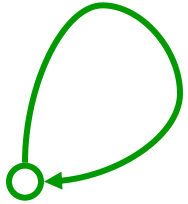


# *Equivalentie- relaties*

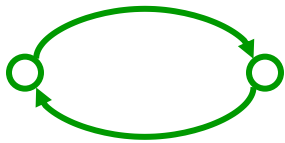


Twaa1fde college

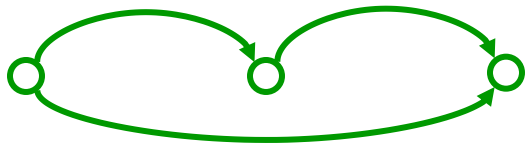




## equivalentie-relaties



reflexief, symmetrisch,  
transitief



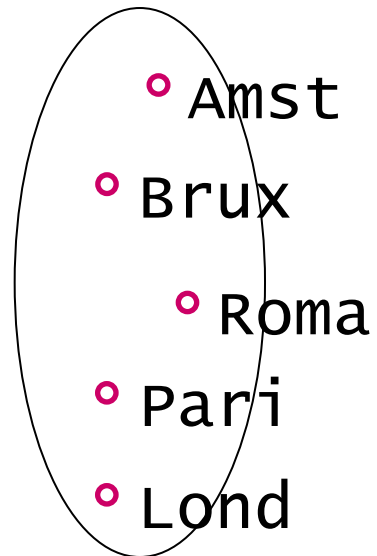
1. gelijkmachtingheid /  
aftelbaarheid
2. modulo rekenen
3. theorie

*Gelijkmatigheid  
en aftelbaarheid*

3.7

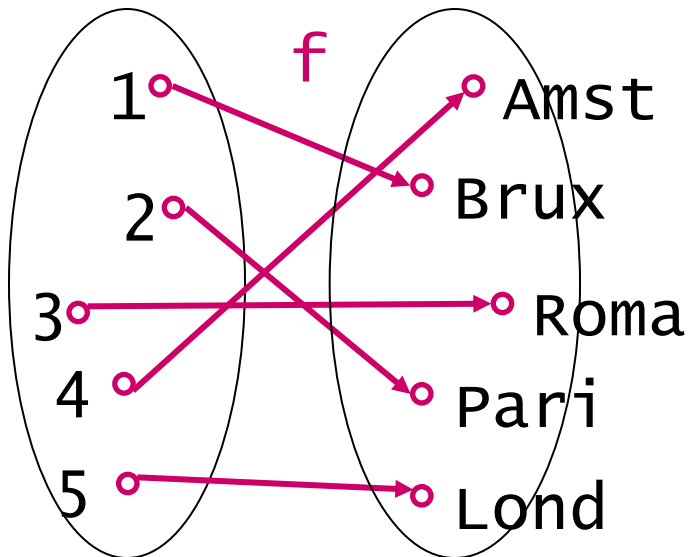
ook: dictaatje §3.2

aleph



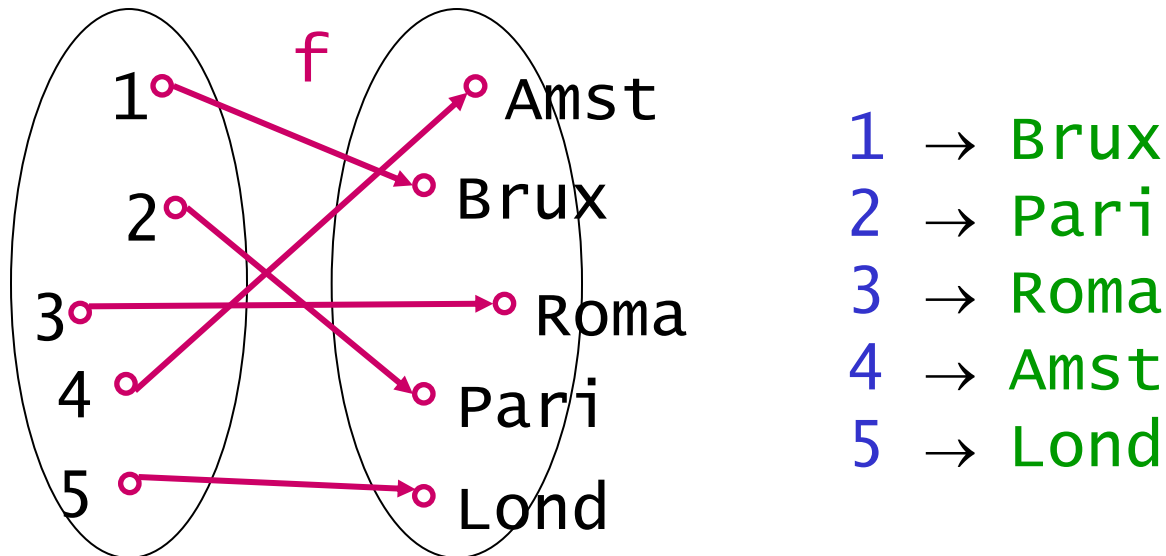
intuïtie

tellen



A eindige verzameling.

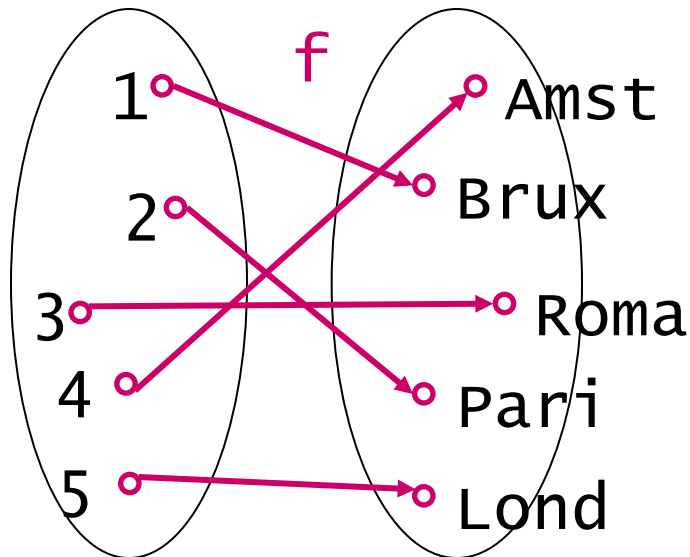
tellen van de elementen van  $A$  is het geven van een bijectie tussen  $\{1, 2, \dots, n\}$  en  $A$ .



Een eindige verzameling  $A$  heeft dus  $n$  elementen  $\Leftrightarrow$  er bestaat een bijectie van  $\{1, 2, \dots, n\}$  naar  $A$ .

A eindige verzameling.

tellen van de elementen van  $A$  is het geven van een bijectie tussen  $\{1, 2, \dots, n\}$  en  $A$ .



1 → Brux  
 2 → Pari  
 3 → Roma  
 4 → Amst  
 5 → Lond

Hoe zit het met oneindige verzamelingen ?  
 'meer/evenveel elementen'  $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$

# Hilberts hotel





$\mathbb{Z}$

... -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 ...

$\mathbb{N}$

0 1 2 3 4 5 6 7 ...

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

bijectie tussen  $\mathbb{N} = \{ 0, 1, 2, 3, \dots \}$  en  $\mathbb{Z}$

E	0	2	4	6	...				
N	0	1	2	3	4	5	6	7	...
E	0	2	4	6	8	10	...		

Zoiets geldt ook voor de even getallen: dat zijn er minder dan de natuurlijke getallen (gezien als deelverzameling) maar toch evenveel (gezien als **gelijkmachtigheid**).

## gelijkmachtigheid

Twee verzamelingen  $A$  en  $B$  heten *gelijkmachtig* als er een bijectie tussen  $A$  en  $B$  bestaat.

Er bestaat een bijectie tussen  $\mathbb{N}$  en  $\mathbb{Z}$   
Er bestaat een bijectie tussen  $\mathbb{N}$  en  $\mathbb{E}$

$\mathbb{N}$  en  $\mathbb{Z}$ , en  $\mathbb{N}$  en  $\mathbb{E}$  zijn gelijkmachtig

zie ook dictaatje H3 §3.2

op het begrip  
gelijkmachtigheid  
komen we straks terug

$\mathbb{Z}$  en  $\mathbb{E}$  zijn *afteelbaar*.

# oneindig aftelbaar

Er bestaat een bijectie tussen  $\mathbb{N}$  en  $\mathbb{Z}$

$0 \rightarrow 0$   $1 \rightarrow -1$   $2 \rightarrow 1$   $3 \rightarrow -2$   $4 \rightarrow 2$   $5 \rightarrow -3$   $6 \rightarrow 3$  ...

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

## Definitie

Een verzameling  $A$  heet *oneindig aftelbaar* als er een bijectie is van  $\mathbb{N}$  naar  $A$ .

$A$  is *aftelbaar* als  $A$  eindig is of oneindig aftelbaar

$\mathbb{Z}$  is aftelbaar.

0 1 2 3 4 5 6 7 8 9 10 11 12 13 ...

1/1 2/1 3/1 4/1 5/1 6/1 ...

1/2 2/2 3/2 4/2 5/2 6/2 ...

1/3 2/3 3/3 4/3 5/3 6/3 ...

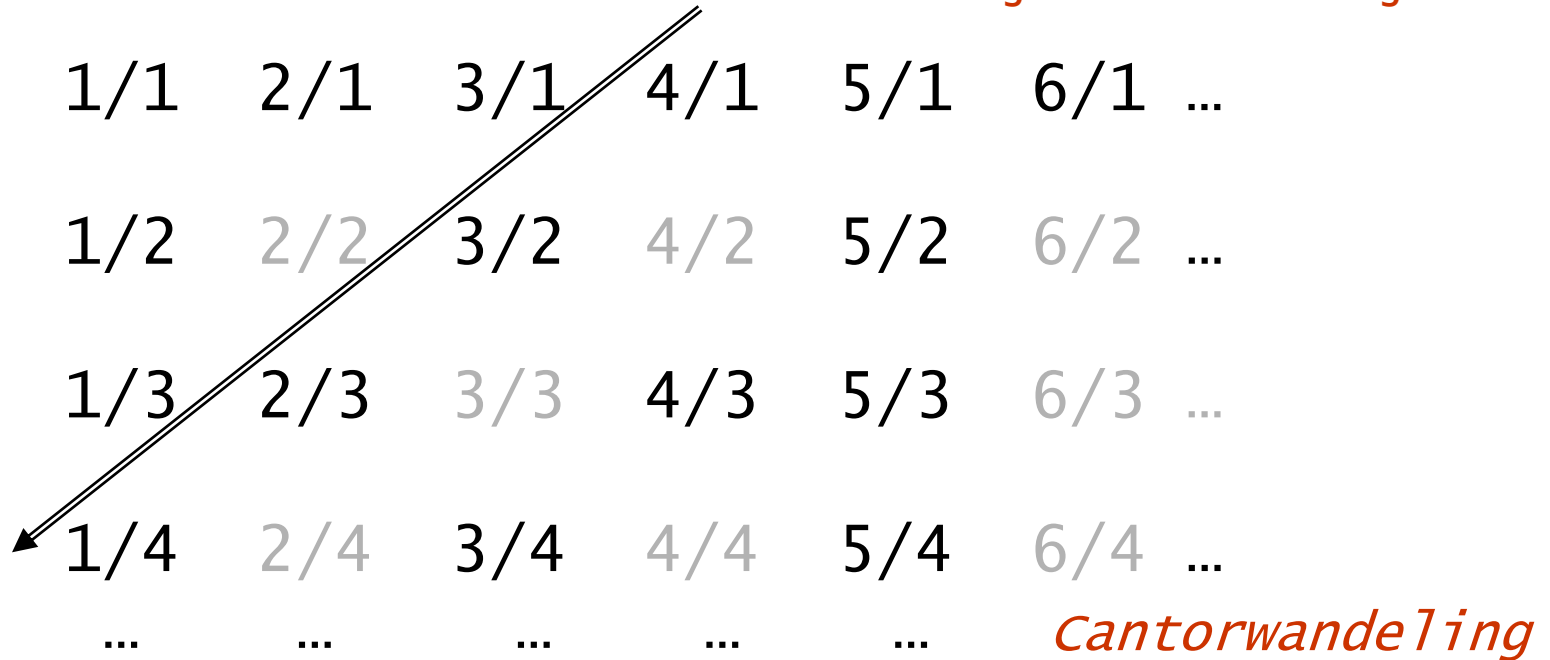
1/4 2/4 3/4 4/4 5/4 6/4 ...

... ... ... ... ...

# breuken zijn aftelbaar

Er bestaat een bijectie tussen  $\mathbb{N}$  en  $\mathbb{Q}^+$

0 1 2 3 4 5 6 7 8 9 10 11 12 13 ...  
1, 2, 1/2, 3, 1/3, 4, 3/2, 2/3, 1/4, 5, 1/5, 6, 5/2, 4/3,  
surjectie vs. bijectie !



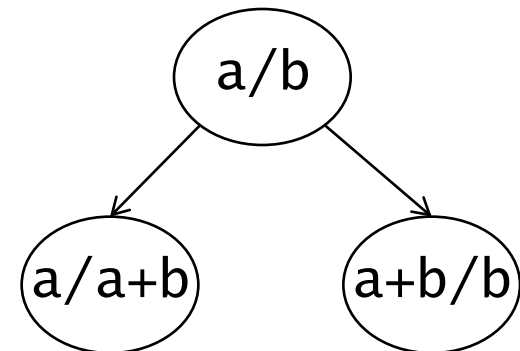
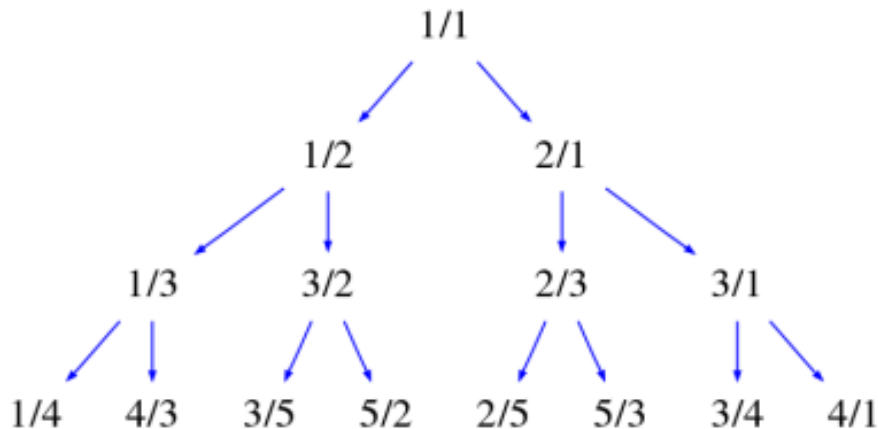
$\mathbb{Q}$  is aftelbaar.

# breuken zijn aftelbaar

Er bestaat een bijectie tussen  $\mathbb{N}$  en  $\mathbb{Q}^+$

**Calkin-wilf**. Ander bewijs: oneindige binaire boom waarin elke (positieve) breuk **precies één keer** voorkomt.

Voordeel: geen herhalingen, toch super-simpel.  
Nadeel: hoe weten we die 'precies één keer'?



Calkin, N. and wilf, H. S. "Recounting the Rationals." *Amer. Math. Monthly* 107, 360-363, 2000.



$f: \mathbb{N} \rightarrow A$

zie volgende slides ...

formeel: aftelbaar  $\Leftrightarrow$  bijectie  
surjectie  $\approx$  'aftelling met herhaling'  
máár ... herhalingen kun je verwijderen

vereniging van twee aftelbare verzamelingen is  
ook aftelbaar: om-en-om  
(en herhalingen verwijderen)

vereniging van aftelbaar veel aftelbare verzamelingen  
is ook aftelbaar: Cantor wandeling

# generalisatie

## surjectie

(oneindig) aftelbaar  $\Leftrightarrow$  bijectie met  $\mathbb{N}$

0	1	2	3	4	5	6	7	8	9	...	$\mathbb{N}$
0	2	0	4	2	6	4	8	6	4	...	surjectie van $\mathbb{N}$ naar $E$

Als een **surjectie**  $f: \mathbb{N} \rightarrow A$  bestaat is  $A$  aftelbaar

vgl. breuken

0	1	2	3	4	5	6	7	8	9	...	$\mathbb{N}$
0	2	4	6	8	10	12	14	16	18	...	bijectie van $\mathbb{N}$ naar $E$

Door herhalingen te verwijderen kun je de surjectie tevens injectief maken

Als een **surjectie**  $f: \mathbb{N} \rightarrow A$  bestaat is  $A$  aftelbaar

0	1	2	3	4	5	6	7	8	9	...	$\mathbb{N}$
0	1	0	1	0	1	0	1	0	1	...	$A$ eindig

geen bijectie mogelijk !

$A$  aftelbaar  $\Leftrightarrow A$  **eindig** of bijectie met  $\mathbb{N}$

$A$  aftelbaar  $\Leftrightarrow$  surjectie van  $\mathbb{N}$  naar  $A$

A aftelbaar:

- eindig
- oneindig: **bijjectie**  $f: \mathbb{N} \rightarrow A$   
 'aftelling' zonder *herhaling*  $f(0), f(1), f(2), \dots$

Als een **surjectie**  $f: \mathbb{N} \rightarrow A$  bestaat is A aftelbaar

Oneindig: bijjectie maken door herhalingen te verwijderen

$$g(0) = f(0)$$

$$g(n) = f(i) \text{ eerste waarde ongelijk aan } g(0), g(1), \dots, g(n-1)$$

vgl. breuken

# generalisatie

## vereniging

$f: \mathbb{N} \rightarrow A$     $g: \mathbb{N} \rightarrow B$    (bijjecties)  
A:    1   2   4   5   7   11   13   17   19   23   ...  
B:    3   5   9   11   15   16   21   23   27   ...

Als  $A$  en  $B$  aftelbaar dan ook  $A \cup B$  aftelbaar

$f: \mathbb{N} \rightarrow A$     $g: \mathbb{N} \rightarrow B$   
om-en-om:     $f(0), g(0), f(1), g(1), f(2), \dots$   
                  0    1    2    3    4    ...  
geeft i.h.a. een **surjectie**  $h: \mathbb{N} \rightarrow A \cup B$

Voor het *voorbeeld*:

0	1	2	3	4	5	6	7	8	9	10	...	$\mathbb{N}$
1	3	2	5	4	9	5	11	7	15	11	...	$A \cup B$

# generalisatie

Als  $A_j$  aftelbaar dan  $\bigcup_{j \in \mathbb{N}} A_j$  aftelbaar

vgl. breuken

$$f_j: \mathbb{N} \rightarrow A_j$$

$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	$f_0(4)$	...
$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	...
$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	...
$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	...
...	...	...	...	...	...

*Cantorwandering*

Als  $A_i$  aftelbaar dan  $\bigcup_{i \in \mathbb{N}} A_i$  aftelbaar (\*)

## Gevolg

De collectie van alle *eindige* deelverzamelingen van  $\mathbb{N}$  is aftelbaar

### Bewijs 1:

$A_i$  = collectie van alle deelverzamelingen ter grootte  $i$   
 Dan is  $A_1$  aftelbaar, dus ook  $A_2$  (waarom?), dus ook  $A_3$ ,  
 etcetera. Derhalve is elke  $A_i$  aftelbaar. Volgens (\*) is  
 $\bigcup_{i \in \mathbb{N}} A_i$  dus aftelbaar.

### Bewijs 2:

$V_i$  = collectie van alle deelverzamelingen bestaande uit  
*hooguit*  $i$  elementen, elk met een waarde tussen 0 en  $i$ .  
 Elke  $V_i$  is eindig (dus aftelbaar) en  $\bigcup_{i \in \mathbb{N}} V_i$  bevat  
 precies alle eindige deelverzamelingen van  $\mathbb{N}$ . Pas nu (\*)  
 toe.

*vergelijk ook opgave 72c*

# overaftelbaar

Er bestaat géén bijectie tussen  $\mathbb{N}$  en  $\mathbb{R}$

(zonder bewijs)

‘diagonalisatie’

probleempje:  $0.9999\dots = 1 = 1.0000\dots$

m.a.w.  $\mathbb{R}$  is niet aftelbaar

*Cantor*

$\mathbb{R}$  is *over*aftelbaar



# diagonalisatie

Men gebruikt “diagonalisatie” om te laten zien dat de reële getallen niet aftelbaar zijn.

Dat heeft technisch een vervelende kant. Je moet eigenlijk weten dat elk rijtje cijfers ‘achter de komma’ een uniek getal vastlegt.

We gaan iets anders doen. We laten zien dat de machtsverzameling van  $\mathbb{N}$  niet aftelbaar is. Sterker: geen enkele machtsverzameling is gelijkmachting met de verzameling zelf!

# diagonalisatie

Er bestaat géén bijectie tussen  $\mathbb{N}$  en  $\mathcal{P}(\mathbb{N})$

$V_0, V_1, V_2, V_3, V_4, V_5, V_6, V_7, \dots$

Bewijs uit het ongerijmde

	0	1	2	3	4	5	6	7	8	9	0	1	2	3	...
$V_0$	+	-	+	-	+	-	+	-	+	-	+	-	+	-	...
$V_1$	-	+	+	+	+	+	-	-	-	-	-	-	-	-	...
$V_2$	-	-	+	+	-	+	-	+	-	-	-	+	-	+	...
$V_3$	-	-	-	-	-	-	-	-	-	-	-	-	-	-	...
$V_4$	-	+	+	+	-	+	-	-	+	-	-	-	-	+	...
$V_5$	+	+	-	-	+	-	-	-	-	+	-	-	-	-	...
$V_6$	+	+	+	+	+	+	-	+	+	+	-	+	-	+	...
...															
$V$	-	-	-	+	+	+	+	...							

$$i \in V \Leftrightarrow i \notin V_i$$

Er bestaat géén bijectie tussen  $\mathbb{N}$  en  $\mathcal{P}(\mathbb{N})$

We bewijzen dit uit het ongerijmde.

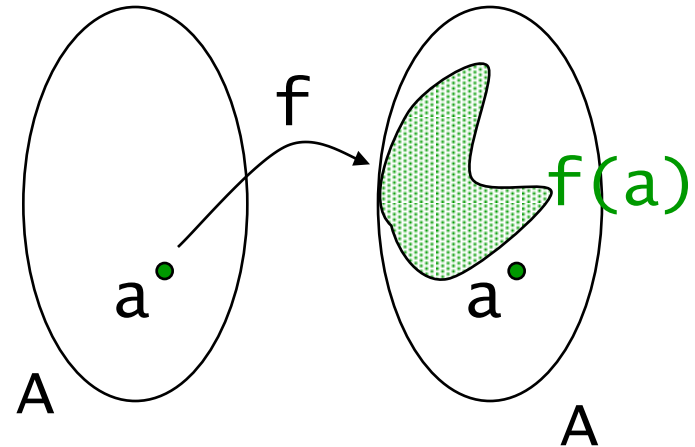
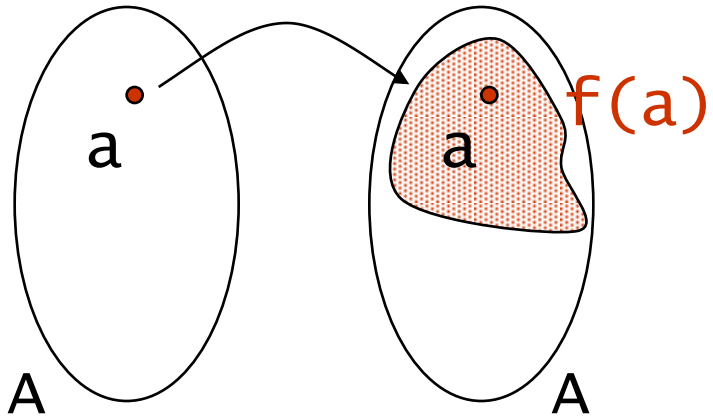
Stel dat er wel een bijectie bestaat; dan kunnen we alle deelverzamelingen van  $\mathbb{N}$  aftellen:  $V_0, V_1, V_2, V_3, V_4, V_5, V_6, V_7, \dots$  met  $V_i \subseteq \mathbb{N}$ .

We kunnen dan een nieuwe verzameling  $V$  construeren die niet in de opsomming voorkomt (zie vorige sheet): immers er geldt voor elke  $i$  dat  $i \in V \Leftrightarrow i \notin V_i$ , dus  $V \neq V_i$  voor elke  $i$ .

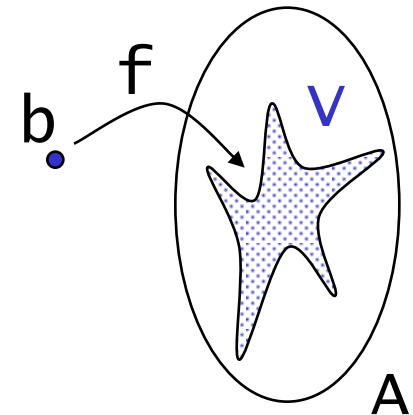
Op de volgende sheets een gegeneraliseerde versie: er bestaat geen bijectie tussen  $A$  en  $\mathcal{P}(A)$ , de machtsverzameling van  $A$ . Het bewijs gaat analoog, ook weer uit het ongerijmde.

# generalisatie: theorem 3.4

Er bestaat géén bijectie tussen  $A$  en  $\mathcal{P}(A)$

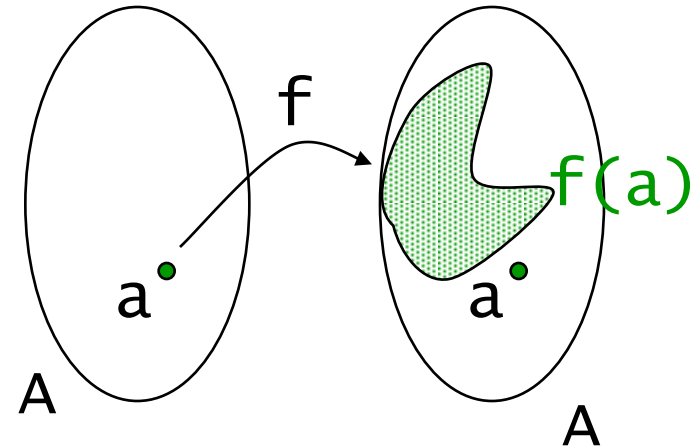
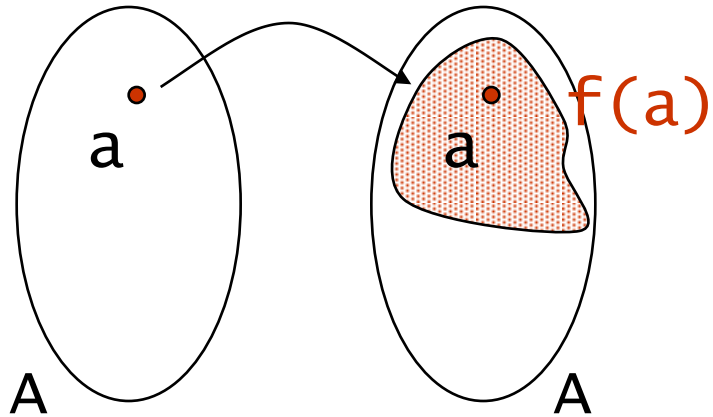


$$V = \{ a \in A \mid a \notin f(a) \}$$



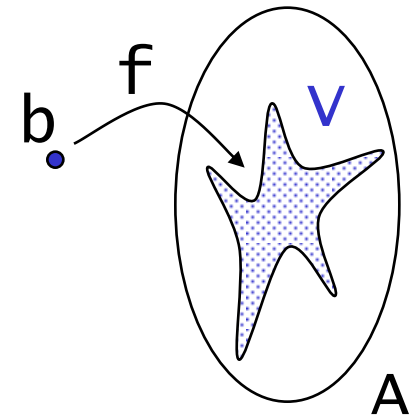
# generalisatie: theorem 3.4

Er bestaat géén bijectie tussen  $A$  en  $\mathcal{P}(A)$



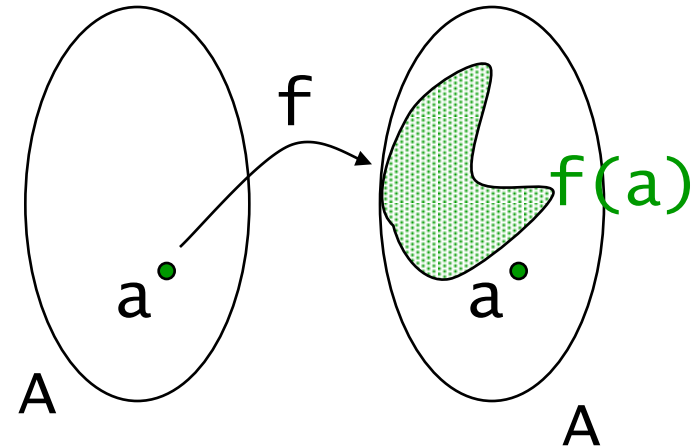
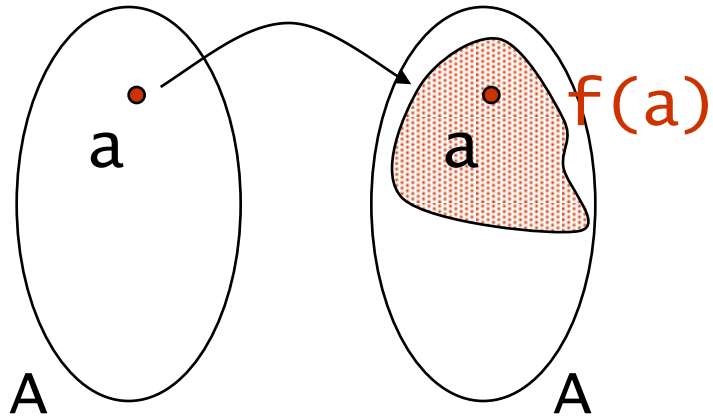
$$V = \{ a \in A \mid a \notin f(a) \}$$

$V \subseteq A$   $f$  surjectief:  $v = f(b)$



# generalisatie: theorem 3.4

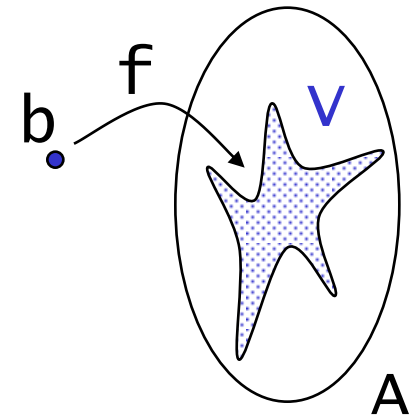
Er bestaat géén bijectie tussen  $A$  en  $\mathcal{P}(A)$



$$V = \{ a \in A \mid a \notin f(a) \}$$

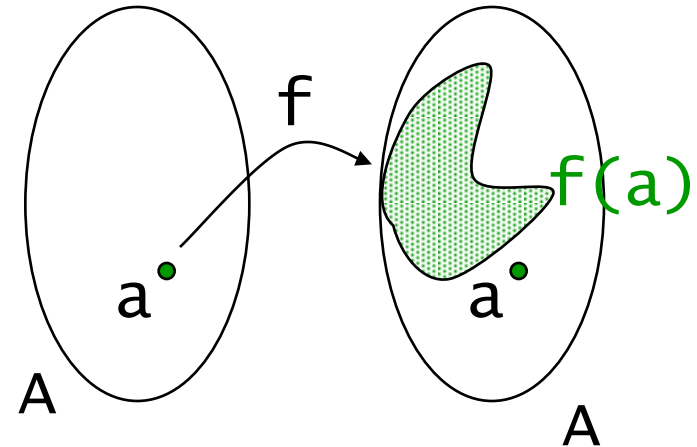
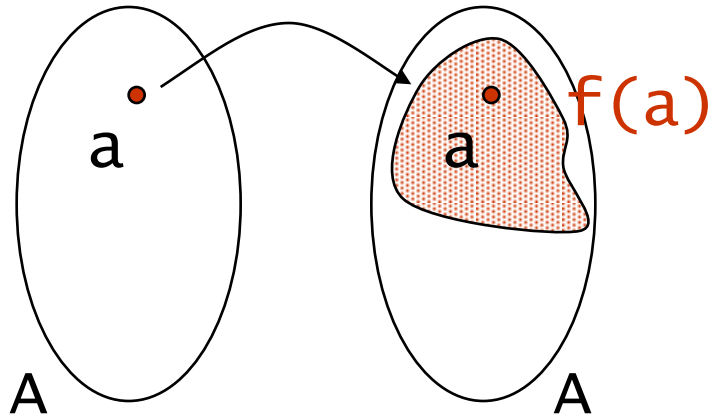
$V \subseteq A$   $f$  surjectief:  $v = f(b)$

$$b \in V \stackrel{\text{def}}{\Leftrightarrow} b \notin f(b)$$



# generalisatie: theorem 3.4

Er bestaat géén bijectie tussen  $A$  en  $\mathcal{P}(A)$



$$V = \{ a \in A \mid a \notin f(a) \}$$

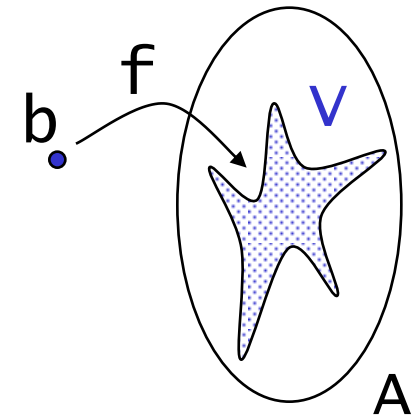
$V \subseteq A$   $f$  surjectief:  $v = f(b)$

$$b \in V \stackrel{\text{def}}{\Leftrightarrow} b \notin f(b)$$

maar  $v = f(b)$  !

$$b \in f(b) \Leftrightarrow b \notin f(b)$$

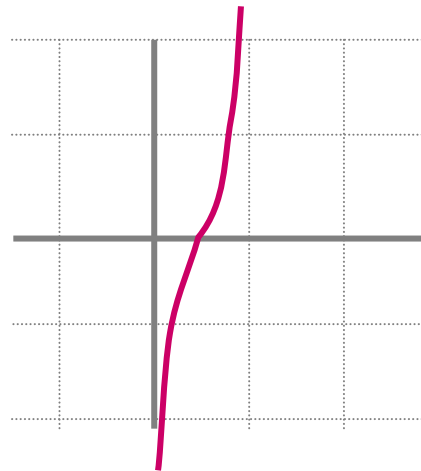
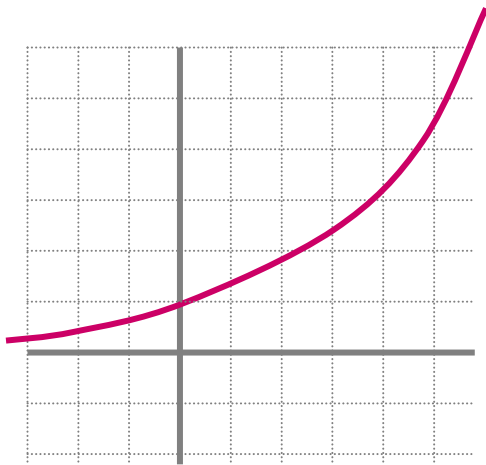
tegenspraak



# gelijkmachtingheid

Twee verzamelingen  $A$  en  $B$  heten *gelijkmachting* als er een bijectie tussen  $A$  en  $B$  bestaat.

Er bestaat een bijectie tussen  $\mathbb{R}$  en  $\mathbb{R}^+$   
Er bestaat een bijectie tussen  $\langle 0, 1 \rangle$  en  $\mathbb{R}$



$\mathbb{R}$  en  $\mathbb{R}^+$ , en  $\langle 0, 1 \rangle$  en  $\mathbb{R}$  zijn gelijkmachting

$A$  en  $\mathcal{P}(A)$  zijn niet gelijkmachting



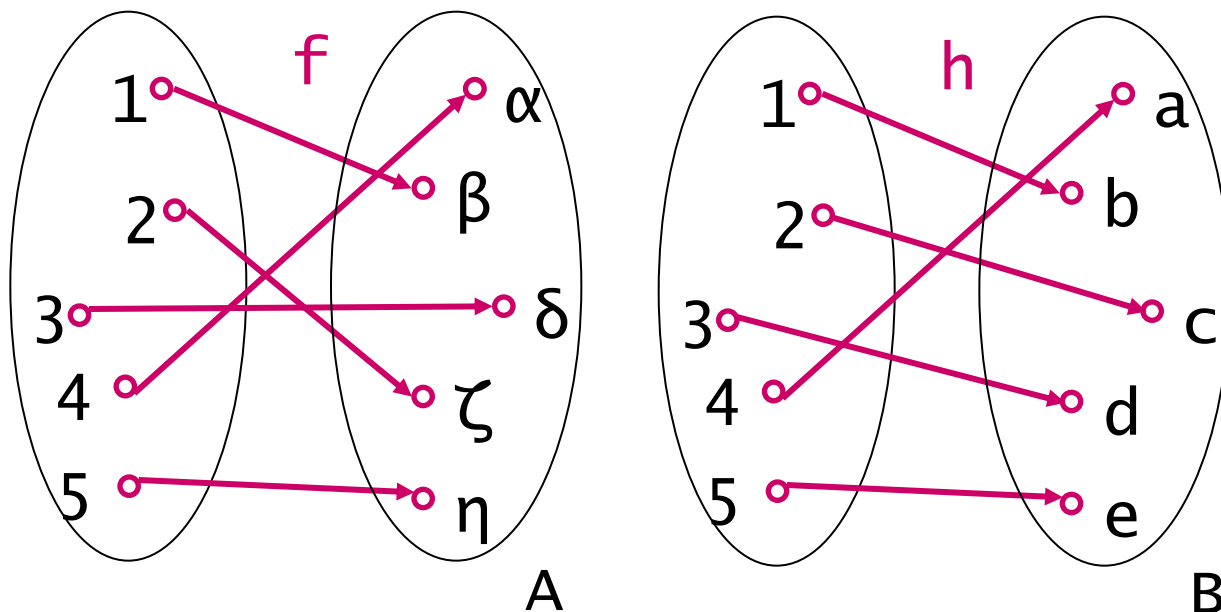
Voor *eindige* verzamelingen A en B geldt: A en B zijn gelijkmachtig desda ze evenveel elementen hebben ( $|A|=|B|$ , of  $n(A)=n(B)$ )

Intuïtief is dit duidelijk, immers een bijectie tussen A en B geeft een 1-1-correspondentie tussen de elementen van A en de elementen van B. Omgekeerd is eenvoudig een bijectie te construeren als het aantal elementen overeenkomt.

Met de formele definitie voor tellen van de elementen van A (bijectie tussen  $\{1, 2, \dots, n\}$  en A) moet eigenlijk ook een formeel bewijs worden gegeven. Zie het dictaatje §3.2, stelling 3.6.

Voor *eindige* verzamelingen A en B geldt: A en B zijn gelijkmachtig desda ze evenveel elementen hebben ( $|A| = |B|$ )

Als voorbeeld van rechts naar links: stel A en B hebben evenveel elementen:  $f$  en  $h$  bijecties



$h \circ f^{-1} : A \rightarrow B$   
bijectie

Twee eindige verzamelingen hebben dezelfde **cardinaliteit** als ze evenveel elementen hebben.

Algemener: twee verzamelingen hebben dezelfde **cardinaliteit** als er een bijectie tussen bestaat, dus als ze **gelijkmachtig** zijn.

Voor oneindige verzamelingen:

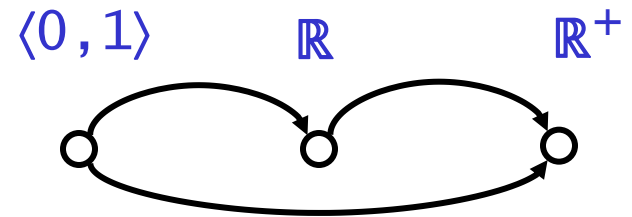
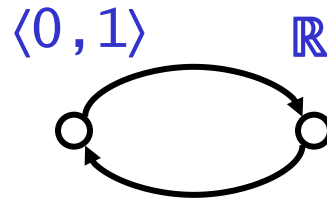
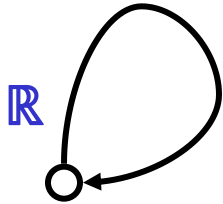
$$|A| = \aleph_0$$

als  $A$  gelijkmachtig is met  $\mathbb{N}$



# gelijkmachtingheid

$\mathbb{R}$  en  $\mathbb{R}^+$ , en  $\langle 0,1 \rangle$  en  $\mathbb{R}$  zijn gelijkmachting



- *reflexief*

$$\text{id} : A \rightarrow A$$

- *symmetrisch*

$$f : A \rightarrow B \text{ dan } f^{-1} : B \rightarrow A$$

- *transitief*

$$f : A \rightarrow B \text{ en } g : B \rightarrow C$$

$$\text{dan } g \circ f : A \rightarrow C$$

Gelijkmachtingheid is dus een **equivalentierelatie**

# paradox van Russell

Er bestaat geen verzameling van alle verzamelingen!

Paradox van Russell.

Laat  $R$  de verzameling zijn van alle verzamelingen die zichzelf niet bevatten:

$$R = \{x \mid x \notin x\}. \text{ Dan geldt: } R \in R \Leftrightarrow R \notin R$$

[http://en.wikipedia.org/wiki/Bertrand\\_Russell](http://en.wikipedia.org/wiki/Bertrand_Russell)

Gerelateerd: Barber paradox.

[http://en.wikipedia.org/wiki/Barber\\_paradox](http://en.wikipedia.org/wiki/Barber_paradox)

# Cantor en Russell



Georg Cantor 1845-1918



Bertrand Russell 1872-1970

# 11.8

*modulo  
rekening*

en dictaatje §3.1

ook: §3.4 modular arithmetic

## §11.8 klokrekenen



17 u.

8 uur later:

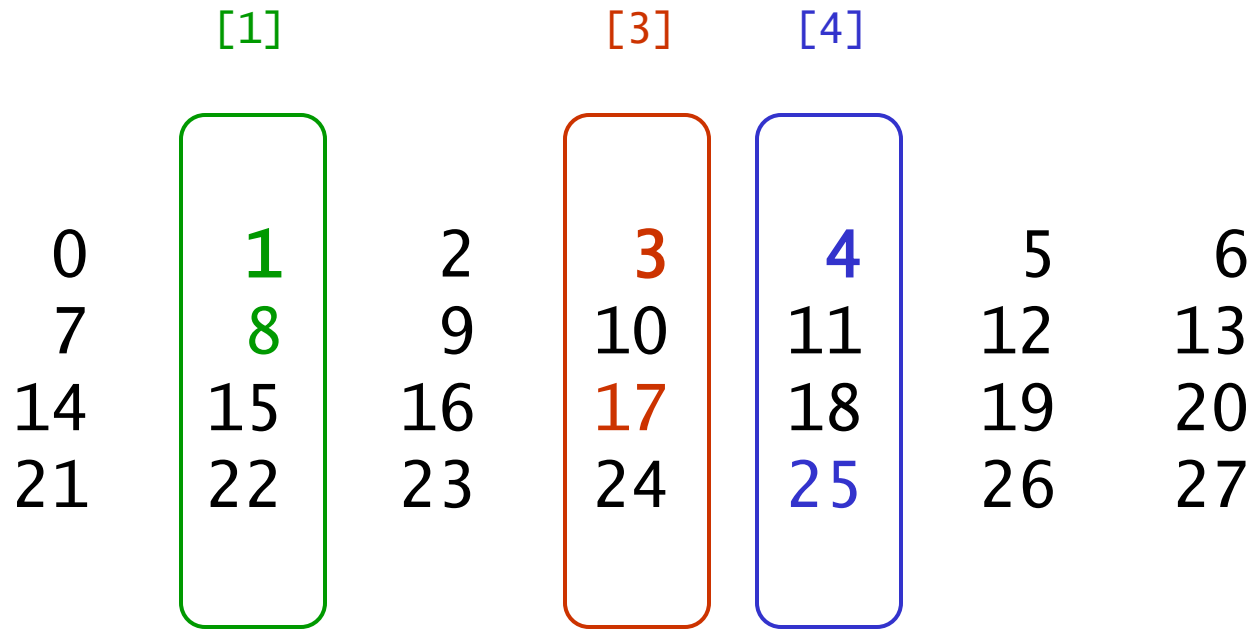
01 u.

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

rekenen modulo 24



# optellen modulo 7



$$\begin{array}{r} 1 + 3 = 4 \\ 8 + 17 = 25 \end{array}$$

$$n \in \mathbb{N}^+$$

$a$  en  $b$  heten *congruent modulo*  $n$   
als  $a-b$  deelbaar is door  $n$

$$a \equiv b \pmod{n}$$

*'dezelfde rest'*  
bij deling door  $n$

Dit is een equivalentierelatie:

- $a \equiv a$

$$a - a = 0$$

- $a \equiv b$  dan  $b \equiv a$

$$b - a = -(a - b)$$

- $a \equiv b$  en  $b \equiv c$  dan  $a \equiv c$

$$a - c = (a - b) + (b - c)$$

$R$  equivalentierelatie,  
dan *equivalentieklasse*  
van  $x$ :  $[x]_R = \{ y \in V \mid xRy \}$

# restklassen

$n \in \mathbb{N}^+$ ;  $a$  en  $b$  heten *congruent modulo*  $n$

als  $a-b$  deelbaar is door  $n$   $a \equiv b \pmod{n}$

De *equivalentieklasse* van  $x$  is  $[x]_{\mathbb{R}} = \{ y \in V \mid x R y \}$

In dit geval:  $[x] = \{ y \in \mathbb{Z} \mid x \equiv y \pmod{7} \}$

## restklassen modulo 7

$$\overline{0} \quad [0] = \{ \dots -14 \quad -7 \quad 0 \quad 7 \quad 14 \quad \dots \}$$

$$\overline{1} \quad [1] = \{ \dots -13 \quad -6 \quad 1 \quad 8 \quad 15 \quad \dots \}$$

$$\overline{2} \quad [2] = \{ \dots -12 \quad -5 \quad 2 \quad 9 \quad 16 \quad \dots \}$$

$$\overline{3} \quad [3] = \{ \dots -11 \quad -4 \quad 3 \quad 10 \quad 17 \quad \dots \}$$

$$\overline{6} \quad [6] = \{ \dots -8 \quad -1 \quad 6 \quad 13 \quad 20 \quad \dots \} = [-8] \quad \text{etc.}$$

## notatie

$$\begin{array}{ccc} -8 \equiv 13 \pmod{7} & \text{of} & \overline{-8} = \overline{13} \\ \text{getallen} & & \text{klassen} \end{array}$$

# equivalentieklassen

*Algemeen:*

Als  $R$  een equivalentierelatie is in een verzameling  $V$ , dan is  $[x]_R$  gedefinieerd als de verzameling van alle elementen uit  $V$  die aan  $x$  “gerelateerd” zijn via  $R$ . Dit noemen we de equivalentieklasse van  $x$ .

Preciezer:

De *equivalentieklasse* van  $x$  is  $[x]_R = \{ y \in V \mid xRy \}$

De collectie van alle equivalentieklassen  $[x]_R$  (genoteerd als  $V/R$ ) is een partitie van  $V$ .

In ons voorbeeld: de restklassen modulo 7 vormen een disjuncte opspanning (partitie) van  $\mathbb{Z}$ . Zie ook verderop en Schaum pagina 32.

# 'congruentie'

als  $a \equiv a'$  en  $b \equiv b'$  (modulo  $n$ )

dan  $a+b \equiv a'+b'$  en  $a-b \equiv a'-b'$  en  $a \cdot b \equiv a' \cdot b'$  (modulo  $n$ )

en  $a^k \equiv (a')^k$  (modulo  $n$ ) (volgt uit  $a \cdot b \equiv a' \cdot b'$ , bv met inductie naar  $k$ )

dus: het maakt niet uit, welk element uit de restklasse gekozen wordt

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

$$72 + 143 = 215 \quad 2 + 3 = 5 \quad \text{maar} \quad 215 \equiv 5$$

$$72 - 143 = -71 \quad 2 - 3 = -1 \quad \text{maar} \quad -71 \equiv -1$$

$$72 \cdot 143 = 10296 \quad 2 \cdot 3 = 6 \quad \text{maar} \quad 10296 \equiv 6$$

bewijs:      want deelbaar door  $n$  ...

$$(a+b) - (a'+b') = (a-a') + (b-b') \equiv 0 \pmod{n}$$

$$(a-b) - (a'-b') = (a-a') - (b-b') \equiv 0 \pmod{n}$$

$$a \cdot b - a' \cdot b' = a(b-b') + b'(a-a') \equiv 0 \pmod{n}$$

# Laatste cijfer

Wat is het laatste cijfer van  $3^{234}$  ?

modulo 10 rekenen

machten van 3

$$1 \quad 3 \quad 9 \quad 3^3=27 \quad 3^4=27 \cdot 3 \equiv 7 \cdot 3 \equiv 1 \pmod{10}$$

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

# weekdagen

1	1	jan	00	za	[1]
2	2	jan	00	zo	[2]
...					
31	31	jan	00		
32	1	feb	00	di	[4]
...					
366	31	dec	00	zo	[2]
...					
xxx	13	mei	23	??	[?]

dagnummers

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

23 jaar · 365 dagen/jaar  
+ 6 schrikkel-dagen  
+ 31+28+31+30+13 dagen in 2023

modulo 7

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

**zaterdag**

# deelbaarheid

voor oneven  $x$ :  
 $x^2-1$  deelbaar door 8

Bewijs?

*basis*

$$8 \mid 1^2 - 1 = 0$$

*inductiestap*

$$(x+2)^2 - 1 =$$

$$x^2 + 4x + 3 =$$

$$x^2 - 1 + 4(x+1)$$

$$8 \mid x^2 - 1 \text{ aanname}$$

$$2 \mid x+1 \text{ (even!)}$$

$$8 \mid 4(x+1)$$

modulo 8 oneven  $x$

$$x^2 - 1 \equiv 0 \text{ dwz } x^2 \equiv 1$$

klassen 1 3 5 7 :

$$1^2 = 1 \equiv 1$$

$$3^2 = 9 \equiv 1$$

$$5^2 = 25 \equiv 1$$

$$7^2 = 49 \equiv 1$$

als  $x \equiv y$   
dan  $x^2 \equiv y^2$

zonder modulo-rekenen:

$$(8k+5)^2 = 64k^2 + 80k + 24 + 1 \text{ is } 8\text{-voud} + 1$$



voor oneven  $x$ :  
 $x^2-1$  deelbaar door 8

Kunnen we bewijzen met volledige inductie, modulo rekenen, ..., hier nog een manier

$$x^2-1 = (x-1)(x+1)$$

Product van twee opvolgende even getallen; dan moet de één deelbaar zijn door 4 en de andere door 2.

m is deelbaar door 9  
als de som van de cijfers van m deelbaar is  
door 9

$$232029 = 25781 \cdot 9$$

$$2+3+2+0+2+9 = 18$$

modulo 9

$$10 \equiv 1$$

$$10^n \equiv 1^n \equiv 1$$

$$c_k \dots c_2 c_1 c_0 =$$

$$c_k 10^k + \dots + c_1 10^1 + c_0 10^0 \equiv$$

$$c_k + \dots + c_1 + c_0$$

$$\sum_{n=0}^k c_n 10^n \equiv \sum_{n=0}^k c_n$$

getal  $\equiv$  som cijfers

# rekenen met restklassen

modulo 6

[1]  $\bar{1}$

+	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

$\mathbb{Z}_6$

‘gewone’ rekenregels:

commutatief, associatief,

distributief, een, nul

maar *niet*  $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$  ‘nuldelers’

$\mathbb{Z}_6$  heeft drie nuldelers: 2, 3 en 4 (eigenlijk  $\bar{2}, \bar{3}, \bar{4}$ )

# rekenen met restklassen

modulo 7

[1]  $\bar{1}$

+	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

$\mathbb{Z}_7$

‘gewone’ rekenregels:  
 commutatief, associatief,  
 distributief, een, nul

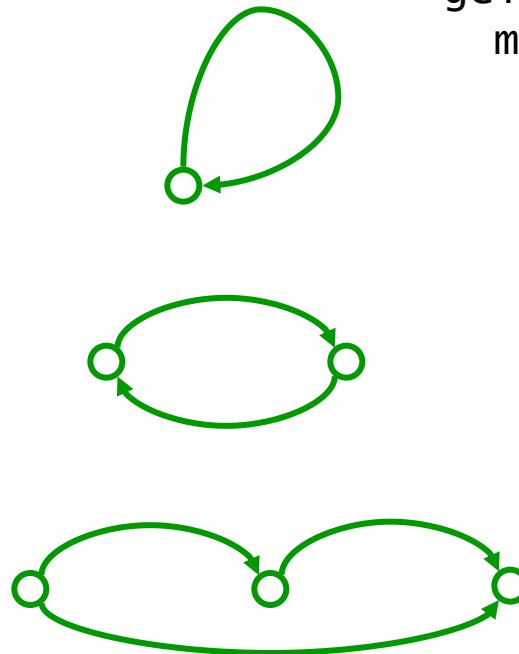
en *wel*  $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$  ‘nuldelers’

$\mathbb{Z}_7$  heeft geen nuldelers

# *Equivalentie- relaties*

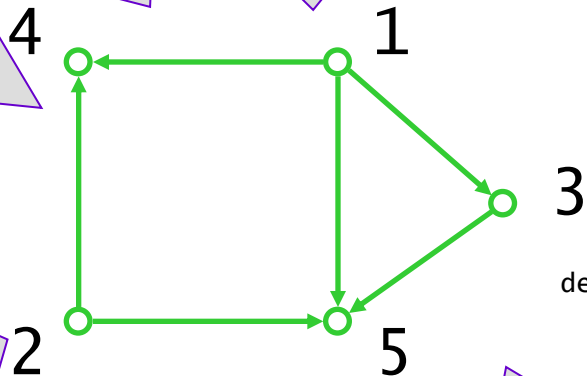
2.8

algemeen  
gelijkmatigheid  
modulo rekening



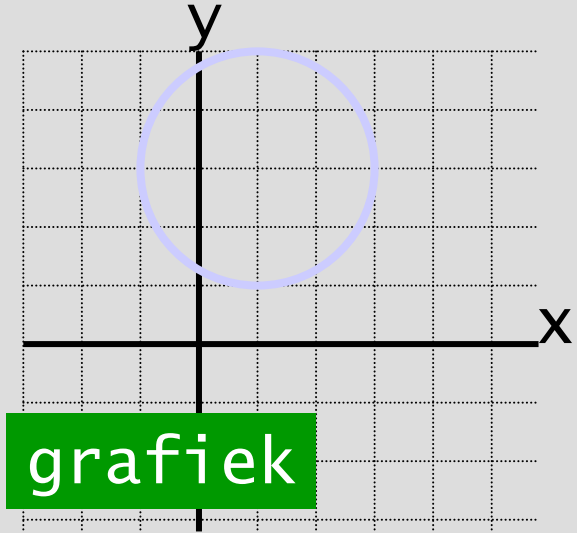
# representaties

van binaire relaties

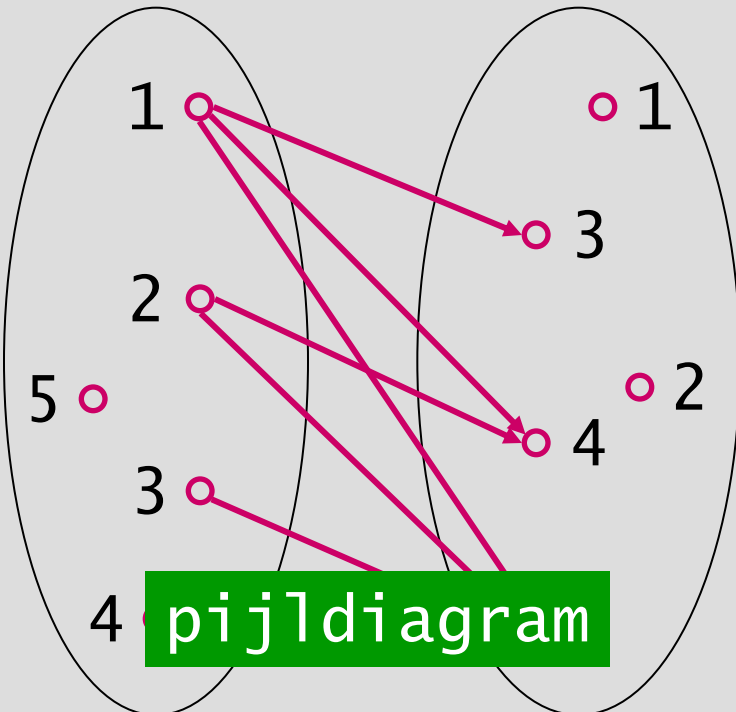


deze gebruiken we

gerichte graaf



grafiek



pijldiagram

		j				
		1	2	3	4	5
i	1	0	0	1	1	1
	2	0	0	0	1	1
	3	0	0	0	0	1
	4	0	0	0	0	0
	5	0	0	0	0	0

matrix

# eigenschappen

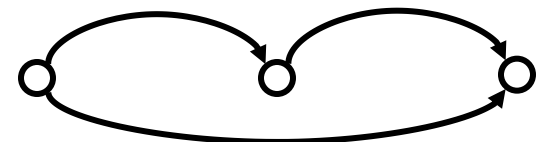
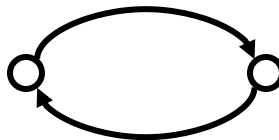
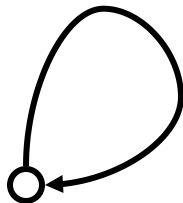
Een relatie  $R \subseteq V \times V$  heet

- *reflexief* als  $xRx$  voor alle  $x \in V$
- *irreflexief* als  $xRx$  voor geen  $x \in V$

- *symmetrisch* als  $xRy$  impliceert dat  $yRx$   
( voor alle  $x, y \in V$  )

- *anti-symmetrisch* als  $xRy$  en  $yRx$  impliceren dat  $x=y$   
( voor alle  $x, y \in V$  )

- *transitief* als  $xRy$  en  $yRz$  impliceren dat  $xRz$   
( voor alle  $x, y, z \in V$  )



## paden in grafen

\*ongericht!

$$p \rightarrow q \quad q \rightarrow r \Rightarrow p \rightarrow r$$

$$p \rightarrow p$$

$$p \rightarrow q \Rightarrow q \rightarrow p \quad (*)$$

samenhangscomponent

## breuken

$$1/2 = 2/4 = 3/6 = \dots$$
$$(1, 2) \sim (2, 4) \sim (3, 6)$$

## gelijkmatigheid

$$f: A \rightarrow B \quad g: B \rightarrow C \Rightarrow g \circ f: A \rightarrow C$$

$$f: A \rightarrow B \Rightarrow f^{-1}: B \rightarrow A$$

$$\text{id}: A \rightarrow A$$

## modulo n

$$x \equiv x \pmod{n}$$

$$x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$$

$$x \equiv y \pmod{n}, y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$$

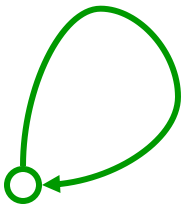


## §2.8 equivalentie

Een relatie  $R \subseteq V \times V$  heet *equivalentierelatie* als  $R$

- reflexief
- symmetrisch, en
- transitief is

### voorbeelden



gelijkheid

gelijkmachtig

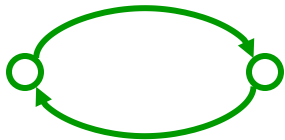
(verzamelingen)

breuken

(paren gehele)

zelfde letters

(strings)



congruentie

(figuren)

evenwijdig

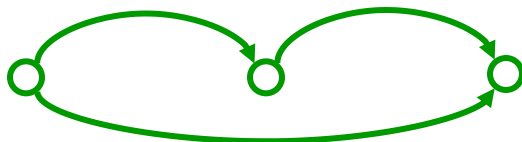
(lijnen)

gelijke kleur

rest modulo  $n$  (gehele getallen)

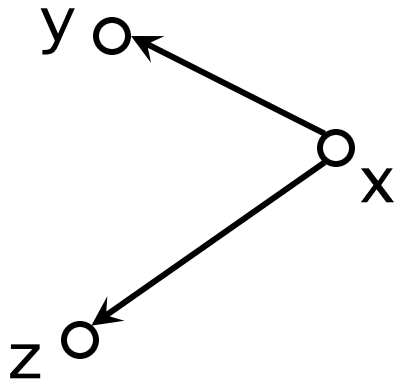
$f: V \rightarrow P$   $f(x) = f(y)$

pad (knopen ongerichte graaf)

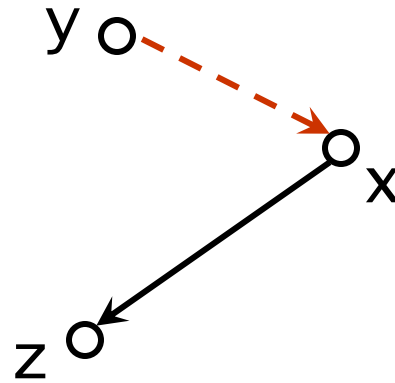


# equivalentieklassen

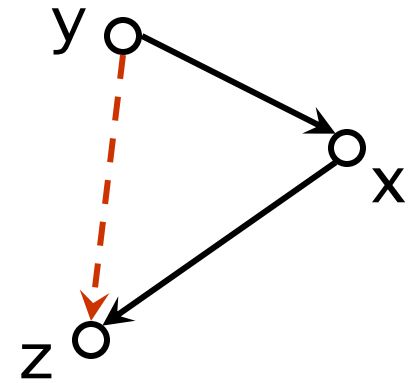
Een relatie  $R \subseteq V \times V$  heet *equivalentierelatie* als  $R$  reflexief, **symmetrisch**, en **transitief** is



als  $xRy$  &  $xRz$



dan  $yRx$



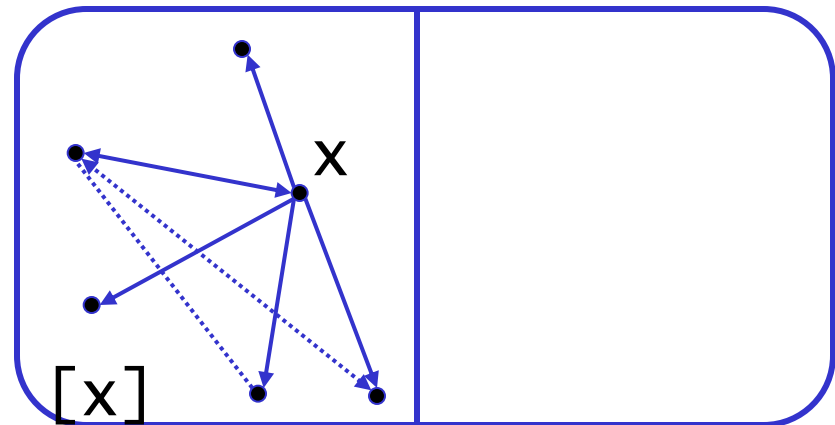
en dus  $yRz$

# Theorem 2.6

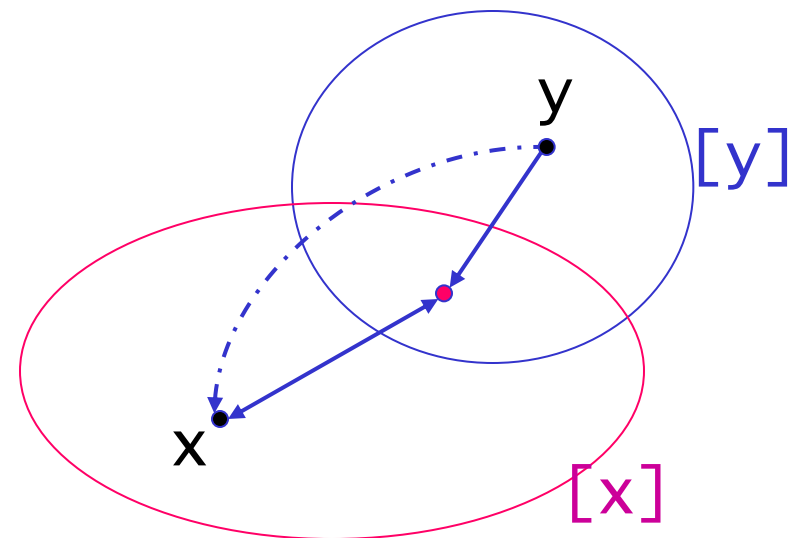
equivalentierelatie: reflexief, symmetrisch, transitief

De *equivalentieklasse* van  $x$  is  $[x]_R = \{ y \in V \mid xRy \}$

partitie!



- $x \in [x]$
- equivalent:
  1.  $xRy$
  2.  $y \in [x]$
  3.  $[x] = [y]$
  4.  $[x] \cap [y] \neq \emptyset$



$\mathbb{Z}$  is gelijk aan de disjuncte vereniging van de zeven restklassen modulo 7. De restklassen modulo 7 vormen dus een partitie van  $\mathbb{Z}$

### restklassen modulo 7

$$\begin{array}{ll}
 [0] & = \{ \dots -14 \ -7 \ 0 \ 7 \ 14 \ \dots \} & 7k \\
 [1] & = \{ \dots -13 \ -6 \ 1 \ 8 \ 15 \ \dots \} & 7k+1 \\
 [2] & = \{ \dots -12 \ -5 \ 2 \ 9 \ 16 \ \dots \} & 7k+2 \\
 [3] & = \{ \dots -11 \ -4 \ 3 \ 10 \ 17 \ \dots \} & 7k+3 \\
 [4] & = \{ \dots -10 \ -3 \ 4 \ 11 \ 18 \ \dots \} & 7k+4 \\
 [5] & = \{ \dots -9 \ -2 \ 5 \ 12 \ 19 \ \dots \} & 7k+5 \\
 [6] & = \{ \dots -8 \ -1 \ 6 \ 13 \ 20 \ \dots \} & 7k+6
 \end{array}$$

# equivalentieklassen

De *equivalentieklasse* van  $x$  is  $[x]_R = \{ y \in V \mid xRy \}$

- **kleur**

$[b]$  blokken met gelijke kleur als  $b$   
wordt bepaald door *kleur*

- **gelijke rest na deling door 7**

$[3] = \{ \dots, -11, -4, 3, 10, 17, \dots \}$   
bepaald door **rest** : 7 klassen

$[0] = \{ \dots, -14, -7, 0, 7, 14, \dots \}$   
*zeven-vouden*

- **afstand tot oorsprong  $\mathbb{R}^2$**

$(x_1, y_1) R (x_2, y_2)$  als  $x_1^2 + y_1^2 = x_2^2 + y_2^2$   
 $[ (2, 1) ]$  alle punten op **afstand  $\sqrt{5}$**   
*cirke!s* !

## nog meer voorbeelden

De *equivalentieklasse* van  $x$  is  $[x]_R = \{ y \in V \mid xRy \}$

- **gelijkmachtigheid**

$[\mathbb{N}]$  verzamelingen gelijkmatig met  $\mathbb{N}$

... *afteelbaar*

$[\mathbb{N}] = [\mathbb{Q}]$  maar  $[\mathbb{R}] \neq [\mathbb{Q}]$

$[\emptyset] = \{ \emptyset \}$

$[\{1, 2, 3, 4, 5\}]$  verz<sup>n</sup> met 5 elementen

*cardinaalgetallen*

- **evenwijdigheid**

$[\ell]$  lijnen evenwijdig met  $\ell$

bepaald door *richtings*-coëfficiënt

- **verbonden door wandeling/pad** (ongericht)

$[p]$  punten verbonden met  $p$ : *component* van  $p$

College volgende week:

dinsdag 4 december,

13.30 – 15.15 in zaal DS (Huygens)

Werkcollege deze week

vrijdag 30 november,

9.00 – 10.45 in Snelliuszalen 402, 405