FACULTEIT INGENIEURSWETENSCHAPPEN
EN ARCHITECTUUR

Hoofdstuk 1 – Inleiding en basisbegrippen

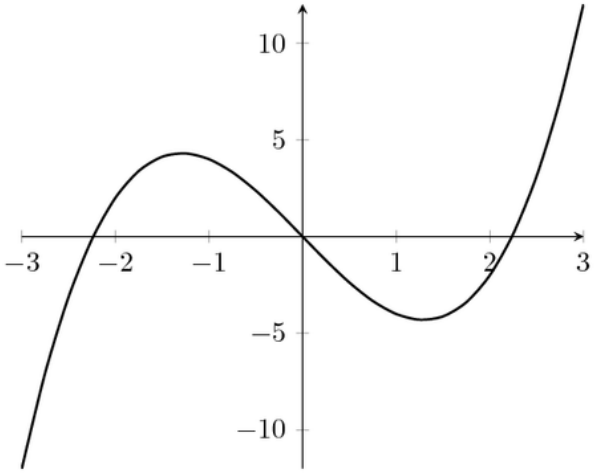
Discrete wiskunde

dr. ir. Cedric De Boom
IDLab - imec

UNIVERSITEIT GENT
IDLab INTERNET & DATA LAB
imec

Wat is discrete wiskunde?

VS



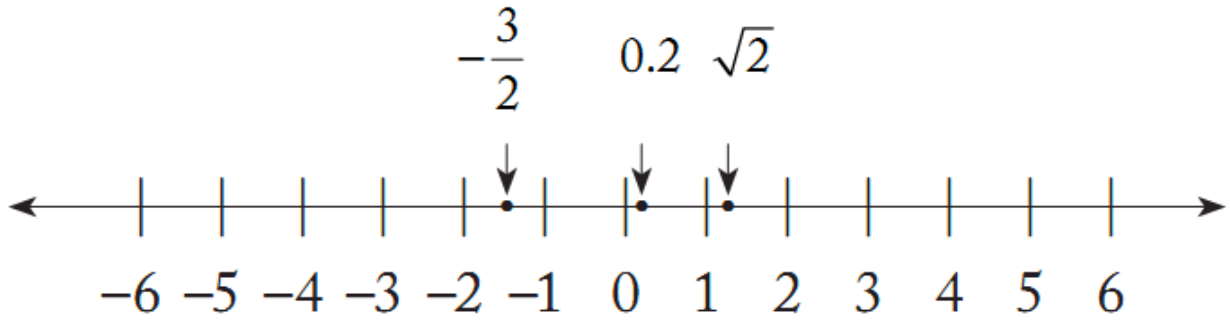
1,34736243244237856273342572364834242347823965732846342103874726391024633437585784673234937565436761248367503745325683274896975435899039747364…

Wat is discrete wiskunde?

Discreet = “afzonderlijk” of “niet verbonden”

Een stap meer of minder heeft betekenis, iets daartussen niet

- Het tellen van objecten
- Het oplossen van logische problemen (waar of vals)
- Het rekenen met gehele getallen
- Het bestuderen van discrete structuren (met eindig of telbaar aantal elementen)
- Het oplossen van recursies
- …



Toepassingen van discrete wiskunde

- Elektronica
- Communicatie
- Cryptografie
- Codeertheorie
- Muziek
- Hardware design
- Signaalverwerking
- Parallel en gedistribueerd rekenen
- Beeldverwerking
- Ontwerp en analyse van algoritmen
- Generatie van random getallen
- Foutopsporing en anomaliedetectie
- …

Een korte geschiedenis

- **Natuurlijke getallen**: origine van de wiskunde
- **Babyloniërs** (3000 vC): 60-tallig talstelsel
- **Aristoteles** (400 vC): logica
- **Euclides** (300 vC): getaltheorie, axiomatische opbouw
- **Al-Khwarizmi** (9e eeuw): cijfer 0
- **Fermat** (17e eeuw): $x^n + y^n = z^n$ ($n > 2$) heeft geen oplossingen (“bewijs in kantlijn”)
- **Euler** (18e eeuw): grafen, priemgetallen, ...
- **Leibniz** (18e eeuw): logica
- **Laplace** (18e eeuw): combinatieleer
- **Gauss** (19e eeuw): oplossen vergelijkingen
- ...
- **20e eeuw**: opkomst elektronica en computer

Discrete vs. numerieke wiskunde

Numerieke wiskunde

= de studie van algoritmes voor het oplossen van problemen in de *continue* wiskunde

Bijvoorbeeld:

- Integratietechnieken
- Het oplossen van differentiaalvergelijkingen
- Het oplossen van vergelijkingen en stelsels
- Interpolatie en regressie
- …

Natuurlijke getallen

Definitie en notatie

$$\mathbb{N} = \{0,1,2,3,4, \dots\}$$
$$\mathbb{N}_0 = \{1,2,3,4, \dots\}$$

Het feit of 0 een natuurlijk getal is, is een afspraak

Eigenschappen

- Gesloten onder $+$ en $\times$
- Niet gesloten onder $-$ en $/$
- Bezit een natuurlijke ordening $<$
  - Elk getal uit $\mathbb{N}$ bezit een opvolger
  - Is dus ideaal voor het beschrijven van rijen, iteratie en recursie: van groot belang voor informatica!

Gehele getallen

Definitie en notatie

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Eigenschappen

- $\mathbb{Z}$ is een **ring**: gesloten onder $+$, $\times$ én $-$ (zie bijlage A in de cursus)
- Niet gesloten onder $/$
- Geen “inductie-eigenschap” meer (zoals bij $\mathbb{N}$)

Groep

Een **groep** is een niet-ledige verzameling $\mathcal{G}$ met een binaire operator $\oplus$ waarvoor geldt:

- $\mathcal{G}$ is **gesloten** onder $\oplus$

  $\forall a, b \in \mathcal{G}: a \oplus b \in \mathcal{G}$
- $\oplus$ is **associatief**

  $\forall a, b, c \in \mathcal{G}: (a \oplus b) \oplus c = a \oplus (b \oplus c)$
- Er is een **uniek eenheidselement** voor $\oplus$

  $\exists e \in \mathcal{G}: \forall a \in \mathcal{G}: a \oplus e = a = e \oplus a$
- Elk element heeft een **invers** voor $\oplus$

  $\forall a \in \mathcal{G}: \exists b \in \mathcal{G}: a \oplus b = e = b \oplus a$

Commutatieve of Abelse groep

Een **commutatieve** of **Abelse groep** is een groep $(\mathcal{G}, \bigoplus)$ waarvoor bijkomend geldt:

- $\bigoplus$ is **commutatief**

  $\forall a, b \in \mathcal{G}: a \bigoplus b = b \bigoplus a$

Ring

Een **ring** is een verzameling $\mathcal{R}$ met twee binaire operatoren $\oplus$ en $\odot$ waarvoor geldt:

- $\mathcal{R}$ is **gesloten** onder $\oplus$
- $\oplus$ is **associatief**
- $\oplus$ is **commutatief**
- Er is een **uniek eenheidselement** voor $\oplus$
- Elk element heeft een **invers** voor $\oplus$

- $\mathcal{R}$ is **gesloten** onder $\odot$
- $\odot$ is **associatief**
- $\odot$ is **distributief** t.o.v. $\oplus$

$$\forall a, b, c \in \mathcal{R}: a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

Uitbreidingen van ringen

Een **commutatieve ring** is een ring $(\mathcal{R}, \oplus, \odot)$ waarvoor bijkomstig geldt:

- $\odot$ is **commutatief**

Een **ring met eenheidselement** is een ring $(\mathcal{R}, \oplus, \odot)$ waarvoor bijkomstig geldt:

- Er is een **uniek eenheidselement** voor $\odot$

$$\exists \mathbf{1} \in \mathcal{R}: \forall a \in \mathcal{R}: a \odot \mathbf{1} = a = \mathbf{1} \odot a$$

Rationale getallen

Definitie en notatie

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0 \right\}$$

Eigenschappen

- $\mathbb{Q}$ is een **veld**: gesloten onder +, ×, − en / (zie bijlage A in de cursus)
- **Dichte ordening**: tussen elke twee rationale getallen x en y ligt een ander getal $\frac{x+y}{2}$

  Geen unieke opvolger meer

Veld

Een **veld** is een commutatieve ring met eenheidselement $(\mathcal{V}, \oplus, \odot)$ met bijkomende eigenschap:

- Elk element $\neq 0$ heeft een **invers element** voor $\odot$

  $\forall a \in \mathcal{V}: \exists b \in \mathcal{V}: a \odot b = \mathbf{1} = b \odot a$

Reële getallen

Definitie en notatie

$\mathbb{R}$ = alle punten op een (geijkte) lijn: de reële getallenas

Voorbeeld: $\sqrt{2}$ en π zijn reële getallen, maar geen rationale getallen:

irrationale getallen: $\mathbb{R} \setminus \mathbb{Q}$

Eigenschappen

- $\mathbb{R}$ is een **veld**: gesloten onder +, ×, − en / (zie bijlage A in de cursus)

Bewijs: $\sqrt{2}$ is irrationaal

Bewijs uit het ongerijmde

Stel dat $\sqrt{2}$ rationaal is, dan moet dit leiden tot een contradictie of logische fout

$\sqrt{2}$ is rationaal $\Leftrightarrow \sqrt{2} = \frac{a}{b}$ met $a, b \in \mathbb{Z}$ en a, b onderling ondeelbaar

$$\Rightarrow 2 = \frac{a^2}{b^2}$$

$$\Rightarrow 2b^2 = a^2$$

$\Rightarrow a^2$ is even

$\Rightarrow a$ is even

$$\Rightarrow a = 2c,\ c \in \mathbb{Z}$$

$$\Rightarrow a^2 = 4c^2$$

$$\Rightarrow 4c^2 = 2b^2$$

$$\Rightarrow 2c^2 = b^2$$

$\Rightarrow b$ is even, wat niet een contradictie is met "a, b onderling ondeelbaar"

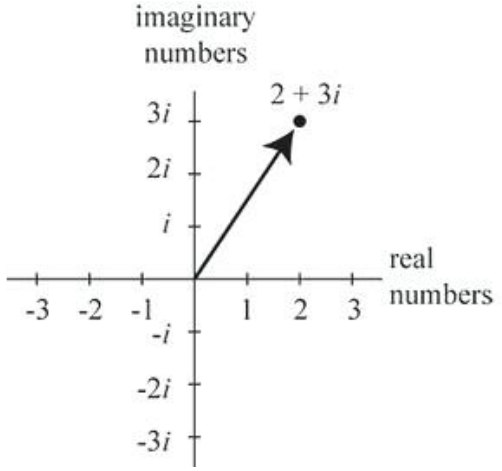
Complexe getallen

Definitie en notatie

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

Eigenschappen

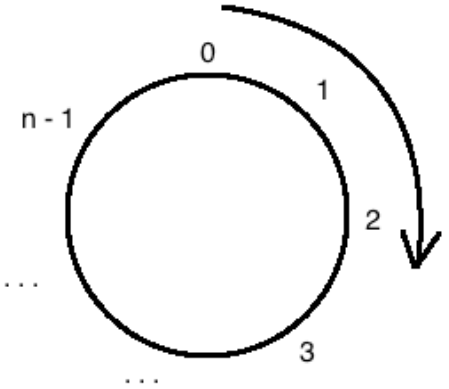
- $\mathbb{C}$ is een **veld**
- Alle veeltermvergelijkingen in 1 onbekende kunnen nu opgelost worden
- Complexe getallen zijn niet meer te ordenen op één lijn
  - Kunnen wel gevisualiseerd worden in een vlak



Gehele getallen modulo n

Definitie en notatie

$$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}, n \in \mathbb{N}, n > 2$$



Eigenschappen

- $+$ en $\times$ verloopt zoals in $\mathbb{Z}$,
  maar de einduitkomst wordt vervangen door de rest bij deling door n
  "*modulo* n"

- In dat geval is $\mathbb{Z}_n$ gesloten onder $+$ en $\times$
  $\mathbb{Z}_n$ is een commutatieve ring met eenheidselement

Optellings- en vermenigvuldigingstabel voor $\mathbb{Z}_8$

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

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Optellings- en vermenigvuldigingstabel voor $\mathbb{Z}_8$

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

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

“nuldelers”

Optellings- en vermenigvuldigingstabel voor $\mathbb{Z}_2$

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Eigenschappen

- Belangrijk voor computertoepassingen (binair)
- $+$ komt overeen met een logische XOR-operatie
- $\times$ komt overeen met een logische AND-operatie

De modulo-operator in programmeertalen

Bijna alle programmeertalen ondersteunen een modulo-operatie
Het gebruikte symbool is meestal %

Let op voor **verschillen**!

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