Proefstuderen Wiskunde

Bewijzen, geheimen, priemgetallen

en waar ze te vinden

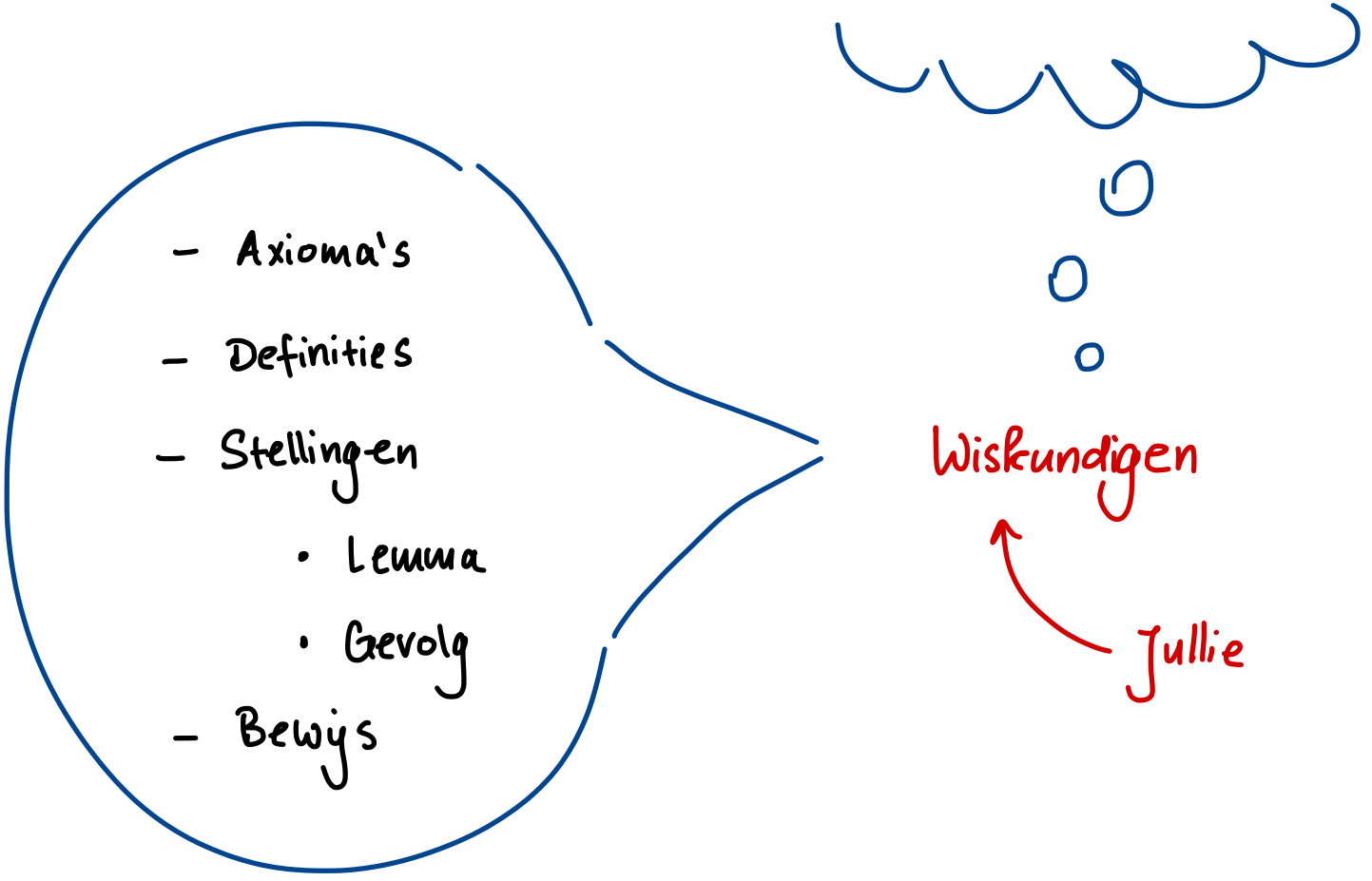
Jeroen Zuiddam

1. Wat is wiskunde?
2. Cryptografie
3. Priemgetallen: bouwstenen van de getalen
4. Priemtest: is een getal priem?
5. Basis-eigenschappen van priemgetallen
6. Modulorekenen
7. Fermat priemtest

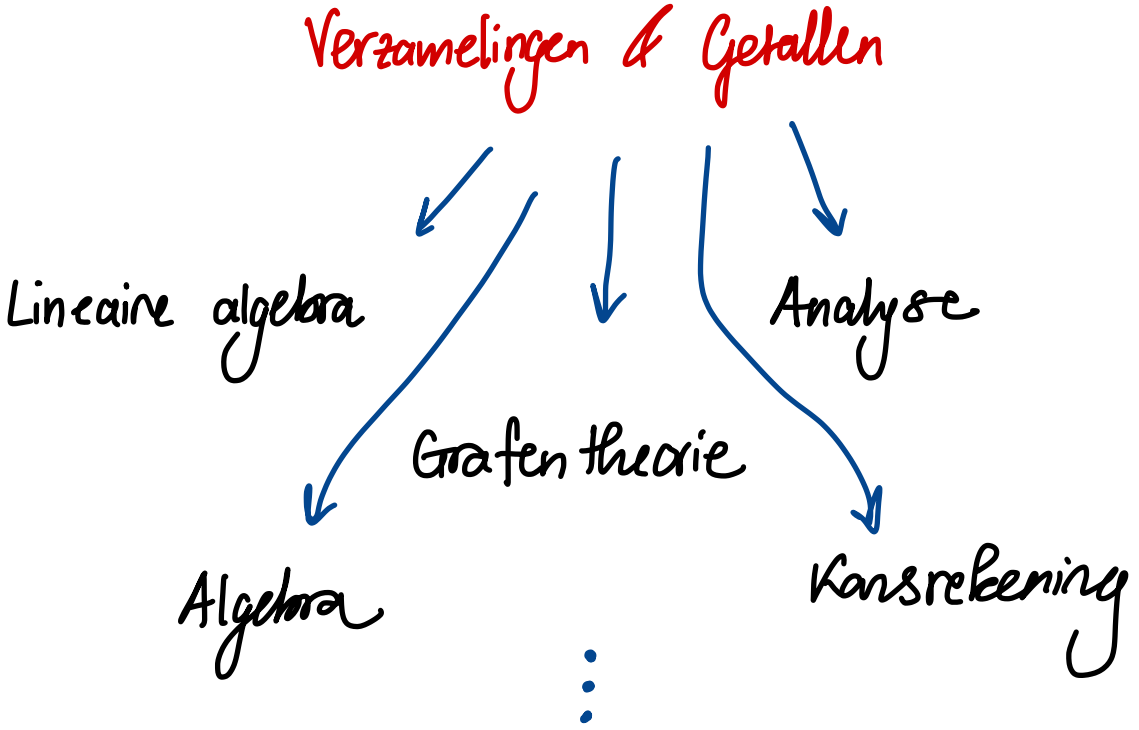
1. Wat is wiskunde?

Wiskunde gaat over de grote vragen:

- Wat is waar? Wat is bewijsbaar?
- Wat zijn de universele structuren in natuur en samenleving?
- Wat zijn de fundamentele mogelijkheden en beperkingen van computers en communicatienetwerken.


- Axioma's
- Definities
- Stellingen
  - Lemma
  - Gevolg
- Bewijs
Wiskundigen
Jullie

Het vak dat ik geef



Algebraïsche meetkunde

Quantum computing

Informatietheorie

Representatietheorie

Universitair onderzoek

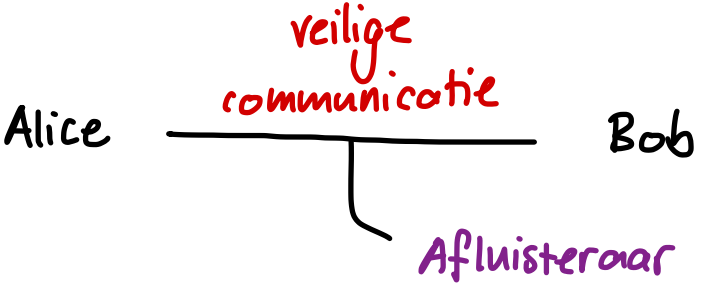
Bedrijfsleven

2. Cryptografie

Doel	Middel
• Een geheim delen	Kluisje, sloten
• Een geheim verifiëren	Vertrouwde derde partij

We willen al dit zonder deze te gebruiken

Wiskunde maakt dit mogelijk!



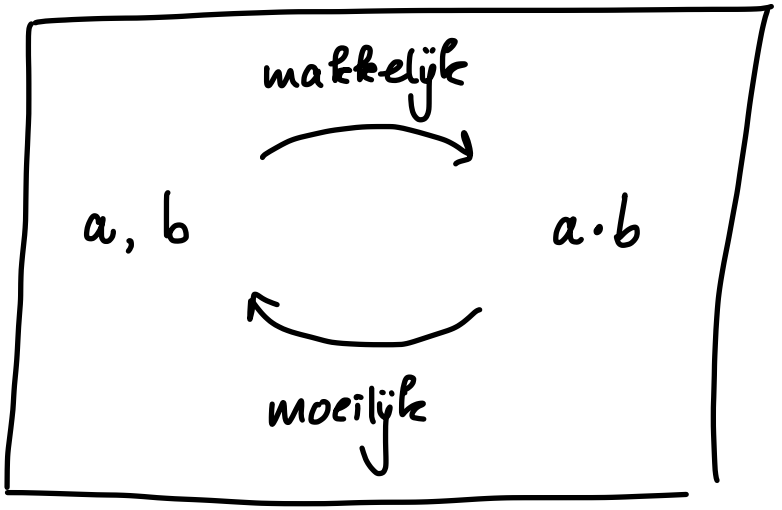
Aannames.

① Beperkte rekenkracht

② Er bestaan makkelijke operaties, die moeilijk zijn om "ongedaan te maken".

② Er bestaan makkelijke operaties, die moeilijk zijn om "ongedaan te maken".

Ontbinden (factoring)



Meer: Discrete logarithm, Hash functies

3. Priemgetallen

- Basisingrediënt voor bijna alle moderne cryptografie
- één van de onderwerpen in mijn rak
- centraal in de wiskunde, al meer dan 2000 jaar
- "bouwstenen" van de getallen
- vinden van "bouwstenen" is belangrijk algemeen thema

Definitie. Zij $n \geq 2$ een natuurlijk getal. We noemen n een priemgetal als 1 en n de enige delers zijn van n.

Voorbeeld 2 3 $4 = 2 \cdot 2$ 5 $6 = 2 \cdot 3$ 7 $8 = 2 \cdot 4$

4. Priemtest

Is 1991 een priemgetal? 1323 ? 6297 ?

Priemtestprobleem: Gegeven een getal n, bepaal snel of n een priemgetal is.

Naief algoritme: Voor elk getal $2 \leq a \leq n-1$:

- als a een deler is van n, zeg: "niet priem"

Anders, zeg: "priem".

5. Basiseigenschappen van priemgetallen

Hoeveel priemgetallen zijn er?

Stelling (Euclides, −300) Er zijn oneindig veel priemgetallen

Bewijs "Bewijs uit het ongerijmde"

Stel er zijn eindig veel priemgetallen $p_1, \ldots, p_k$.

neem $N = p_1 \cdot p_2 \cdots p_k + 1$. Zij $q \geq 2$ het kleinste getal dat N deelt. Dan moet q priem zijn. Dus $q = p_i$ voor een i.

Dan: p_i deelt N en p_i deelt $p_1 \cdot p_2 \cdots p_k$. Dus p_i deelt het verschil $N - p_1 \cdot p_2 \cdots p_k = 1$. Maar $p_i \geq 2$. Tegenspraak!

Stelling (Bertrand)

Voor elke $n \in \mathbb{N}$ is er een priemgetal tussen n en $2n$.

Priemgetallen als "bouwstenen"

Stelling (Hoofdstelling van de rekenkunde, Euclides)

Elk natuurlijk getal kan worden geschreven als product van priemgetallen, en deze schrijfwijze is uniek op volgorde na.

Voorbeeld $6 = 2 \cdot 3 = 3 \cdot 2$

$8 = 2 \cdot 2 \cdot 2 = 2^3$

$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$

Bewijs "Bewijs met inductie"

$n = a \cdot b$

$= (c \cdot d) \cdot (e \cdot f)$

$\vdots$

$= p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$

$12 = 3 \cdot 4$

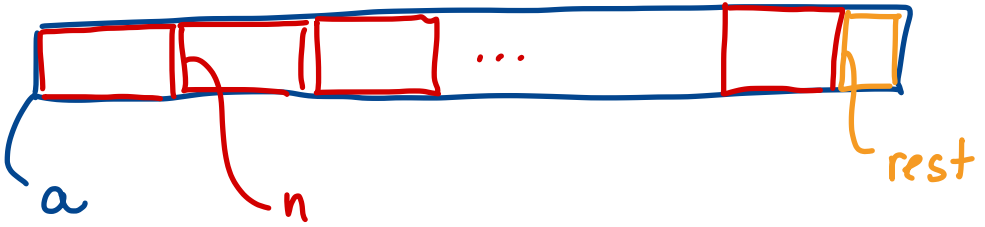
$= 3 \cdot (2 \cdot 2)$

$27 = 3 \cdot 9$

$= 3 \cdot (3 \cdot 3)$

4. Modulorekenen

Gegeven natuurlijke getallen a, n



We definiëren $a \pmod n = \text{rest}$

Voorbeeld

$100 \pmod{10} = 0$

$17 \pmod 2 = 1$

$3 \pmod 4 = 3$

$7 \pmod 4 = 3$

$a \pmod n$ is wat overblijft als we n zo vaak mogelijk van a aftrekken.

4. Fermat priemtest

Een efficiënte test om te bepalen of een getal priem is, die "bijna altijd" werkt.

Kleine stelling van Fermat

Als n priem is, dan geldt voor elk getal $0 \leq a \leq n$ dat $a^n \pmod{n} = a$.

Voorbeeld

$n = 3 \quad a = 2 \quad a^{n-1} = 2^2 = 4 = 1 \mod 3$

$n = 6 \quad a = 2 \quad a^{n-1} = 2^5 = 32 = 2 \mod 6$

Bewijs straks

Kleine Stelling van Fermat

Als n priem is, dan geldt voor elk getal $0 \leq a \leq n$ dat $a^n \pmod n = a$.

↓ Contrapositiere verwoording

Als er een getal $0 \leq a \leq n$ is zodat $a^n \pmod n \neq a$ dan is n niet priem.

Fermat priemtest Gegeven n, kies willekeurig een aantal $0 \leq a \leq n$.

Als steeds $a^n \pmod n = a$: zeg "waarschijnlijk priem"

Ander : zeg "niet priem".

Fermat priemtest Gegeven n, kies willekeurig een aantal $0 \leq a \leq n$.

Als steeds $a^n \pmod n = a$: zeg "waarschijnlijk priem"

Ander : zeg "niet priem".

Opmerkingen

- De test is bijna altijd correct voor willekeurig gekozen n

  → Er zijn waarden van n waar de test faalt, opgave.

- De test is computationeel efficient en gebruikt in de praktijk.
- Er zijn geavanceerdere tests die beter presteren
- In 2002 werd de eerste deterministische (geen willekeurigheid) priemtest gevonden door Agrawal-Kayal-Saxena.

Kleine stelling van Fermat Als n priem is, dan geldt voor elke getal $0 \leq a \leq n$ dat $a^n \pmod n = a$.

Lemma ("Freshman's dream") Voor elke natuurlijke getallen x en y en priemgetal p, geldt $(x+y)^p \pmod p = x^p + y^p \pmod p$

→ Opgave

Bewijs "Bewijs met inductie" De stelling is waar voor $a = 0$.

Stel de stelling is waar voor $a = k$ dus $k^n \pmod n = k$.

We gaan bewijzen dat het waar is voor $a = k+1$.

Bekijk $(k+1)^p$. Het lemma zegt dat $(k+1)^p \pmod p = k^p + 1^p \pmod p$.

De inductiehypothese zegt dat $k^p = k \mod p$.

Dus $(k+1)^p = k+1 \mod p$. □.