

wiskunde en computers: twee revoluties

Freek Wiedijk **Herman Geuvers**

Radboud Universiteit Nijmegen

5 februari 2016
22e nationale wiskundedagen



inhoudsopgaaf

constructieve wiskunde

formele wiskunde

twee revoluties

en een puzzel...

Nederlandse wiskundigen



Christiaan Huygens



L.E.J. Brouwer
constructieve wiskunde



N.G. de Bruijn
formele wiskunde



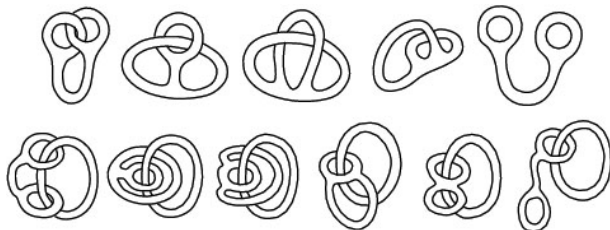
Hendrik Lenstra

L.E.J. Brouwer

Luitzen Egbertus Jan ('Bertus') Brouwer
Overschie 1881 – Blaricum 1966

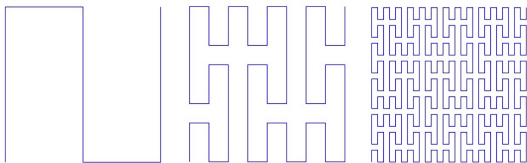
hoogleraar wiskunde aan de
Universiteit van Amsterdam

grondlegger van de **topologie**
meetkunde van de continue vervorming



de lijn versus het vlak

de lijn en het vlak hebben evenveel punten



continue ruimtevullende kromme:

de lijn heeft méér punten dan het vlak

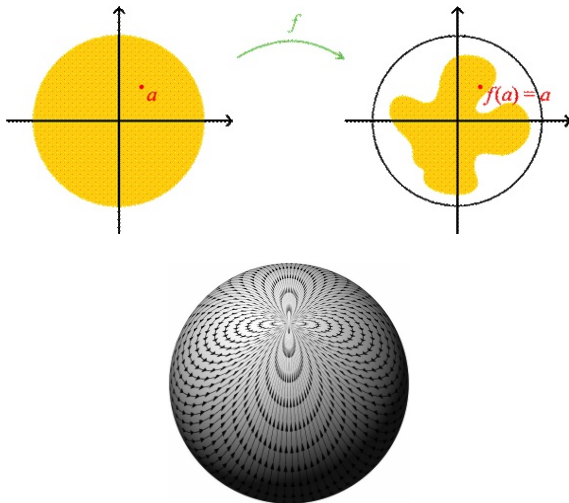
L.E.J. Brouwer:

de lijn en het vlak zijn **topologisch** verschillend

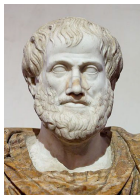
invariantie van domein:

onder continue injectie van $\mathbb{R}^n$ naar $\mathbb{R}^n$ is beeld van open en samenhangende verzameling ('domein') open en samenhangend

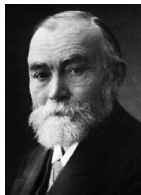
de dekpuntstelling en een bal met haar



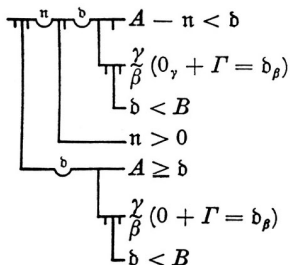
de uitvinding van de logica



Aristoteles
vierde eeuw
voor Christus



Gottlob Frege
negentiende
eeuw



Begriffsschrift

1879

op drift in paradoxen: Russells paradox

$$\{x \mid x \notin x\} \in \{x \mid x \notin x\} ?$$

geldt per definitie precies in het geval dat

$$\{x \mid x \notin x\} \notin \{x \mid x \notin x\}$$

kan niet waar zijn, kan niet onwaar zijn!



Bertrand Russell
1901

Frege's logica uit Begriffsschrift is **inconsistent**

lees: Apostolos Doxiadis & Christos Papadimitriou, *Logicomix*

op drift in paradoxen: de hyperspel paradox

hyperspel:

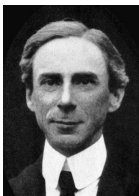


drie scholen



David Hilbert
formalisme

*'spel met
symbolen'*



Bertrand Russell
logicisme

*'komt neer
op logica'*



L.E.J. Brouwer
intuïtionisme

*'constructies
in de geest'*

**constructieve
wiskunde**

Brouwer-Heyting-Kolmogorov interpretatie van formules

Een formule A is waar als er een bewijs voor is

Een bewijs van

$A \wedge B$ is een paar van een bewijs van A en een bewijs van B

$A \vee B$ is een bewijs van A of een bewijs van B

$A \rightarrow B$ is een methode om, gegeven een bewijs van A ,
een bewijs van B te maken

constructief zijn **niet** algemeen geldig:

wet van de uitgesloten derde:

$$A \vee \neg A$$

‘iets is zo, of het is niet zo’

(maar wat als je niet weet welke het geval is?)

dubbele negatie eliminatie:

$$\neg\neg A \Rightarrow A$$

‘als iets niet onwaar kan zijn, dan is het waar’

(maar weet je dan ook waarom?)

een doos met een lampje



voor **iedere** wiskundige vraag kan ik je een doos met lamp geven, waarbij de lamp aan is als het antwoord op de vraag 'ja' is, en waarbij de lamp uit is als het antwoord op de vraag 'nee' is

oplossing:

ik geef **twee** dozen, eentje met lamp aan en eentje met lamp uit
nu heb ik je de beloofde doos gegeven!

voorbeeld van een niet-constructief bewijs

stelling

er bestaan irrationale x en y met x^y rationaal

bewijs

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2$$

als $\sqrt{2}^{\sqrt{2}}$ rationaal, neem $x = y = \sqrt{2}$

als $\sqrt{2}^{\sqrt{2}}$ irrationaal, neem $x = \sqrt{2}^{\sqrt{2}}$ en $y = \sqrt{2}$

QED

constructief **geen bewijs** zonder te bewijzen of $\sqrt{2}^{\sqrt{2}}$ rationaal is
(maar: $\sqrt{2}^{\sqrt{2}}$ is irrationaal)

Intermezzo: (vrijwel) elk rationaal getal is van deze vorm

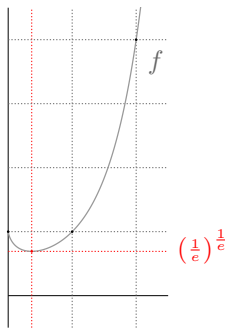
stelling

voor iedere rationale $y \geq \left(\frac{1}{e}\right)^{\frac{1}{e}}$ met $y \notin \{1, 4, 27, 256, \dots\}$
bestaat er een irrationale x met $y = x^x$

bewijs

neem $f(x) = x^x$ dan $f'(x) = x^x(1 + \ln x)$ en dus $f'(\frac{1}{e}) = 0$

voor iedere $y \geq \left(\frac{1}{e}\right)^{\frac{1}{e}}$ is er daarom een x met $y = x^x$



Curry-Howard isomorfisme



Haskell Curry



William Howard

bewijzen corresponderen met **computerprogramma's**

constructieve
wiskunde

functionele
programmeertaal

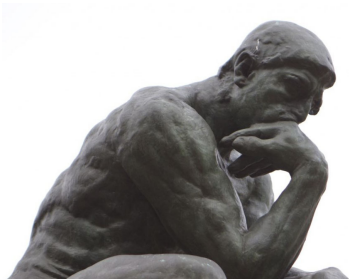
als je constructief bewijst dat iets bestaat heb je ook meteen een computerprogramma om het uit te rekenen

keuzerijtjes

is er voor ieder reëel getal een computerprogramma dat de cijfers van dat getal uitrekent?

L.E.J. Brouwer: nee!

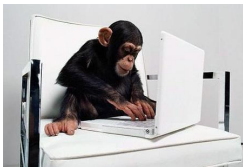
intuïonisme



scheppend subject

de constante van Chaitin

$$\Omega := \left\{ \begin{array}{l} \text{de kans dat een} \\ \text{willekeurig gegenereerd} \\ \text{computerprogramma niet} \\ \text{oneindig blijft doorlopen} \end{array} \right\}$$



Gregory Chaitin
1975

specifieke waarde hangt af van specifieke definities:
wat is een computerprogramma? hoe zijn de kansen?

$$0 < \Omega < 1$$

bijzondere eigenschappen ongeacht precieze definitie

halting probleem

- ▶ Er is geen programma dat het **halting probleem** oplost.
(Gegeven een programma, beslist of het stopt.)
- ▶ Gevolg: Er is geen computerprogramma dat de cijfers van Ω uitrekent,
- ▶ Want: de cijfers van Ω geven een oplossing van het **halting probleem**

Gödels onvolledigheidstelling:

in ieder consistent formeel systeem zijn er ware uitspraken die **niet te bewijzen** zijn specifiek voor Ω :

- ▶ geen enkel formeel systeem kan bewijzen wat de cijfers van Ω zijn (voorbij een zeker punt)



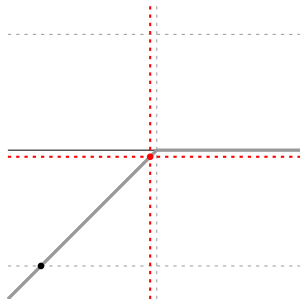
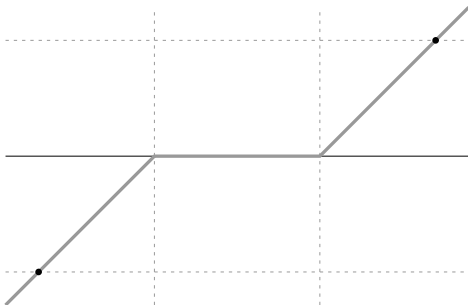
Alan Turing
1936



Kurt Gödel
1931

de tussenwaardestelling

constructief geldt de tussenwaardestelling **niet** in het algemeen (er is geen algoritme dat de tussenwaarde kan uitrekenen).



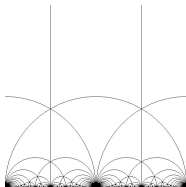
$$\omega \leq 0 \vee \omega \geq 0 ?$$

$$\omega := \left(-\frac{1}{2}\right)^{\text{aantal stappen dat een programma loopt}}$$

N.G. de Bruijn

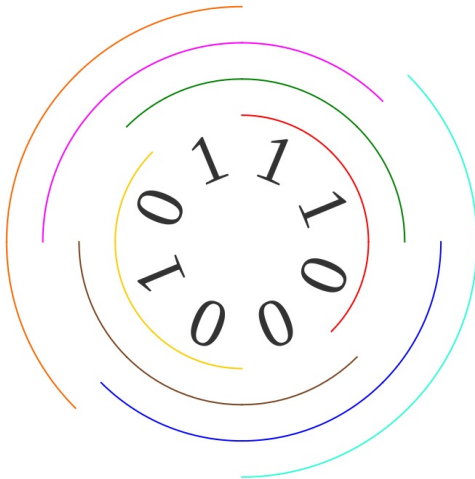
Nicolaas Govert ('Dick') de Bruijn
Den Haag 1918 – Nuenen 2012

hoogleraar wiskunde aan de
Technische Universiteit Eindhoven

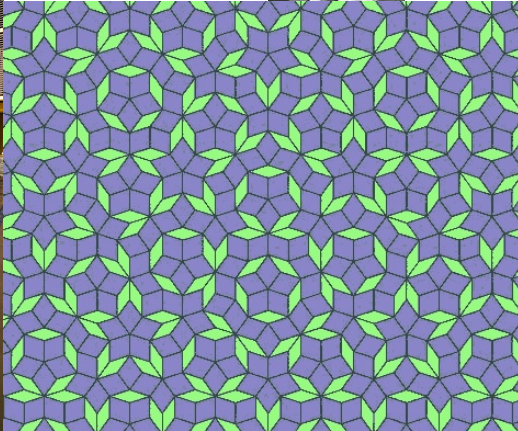
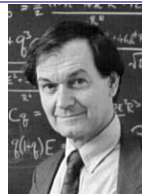
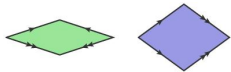


- ▶ modulaire vormen
- ▶ BEST-stelling
(de Bruijn, van Aardenne-Ehrenfest, Smith, Tutte)
formule voor het aantal Euler-cykels in een graaf
- ▶ asymptotische analyse

de Bruijn-rijtje

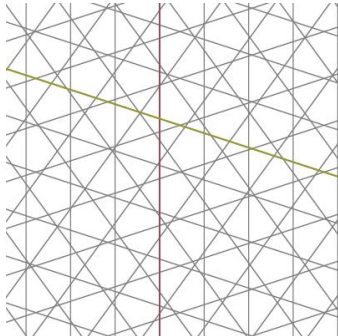
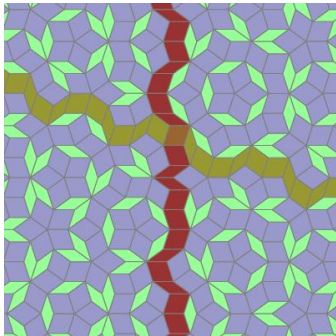


Penrose-betegelingen en quasikristallen



pentagrids

N.G. de Bruijn:



Principia Mathematica

reconstructie van de **wiskunde**
gecodeerd **als formele logica**

drie delen

1910, 1912, 1913



Alfred North
Whitehead



Bertrand
Russell

fragment van pagina 379:

***54.43.** $\vdash :: \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54.26 . \supset \vdash :: \alpha = \iota'x . \beta = \iota'y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

[*51.231] $\equiv . \iota'x \cap \iota'y = \Lambda .$

[*13.12] $\equiv . \alpha \cap \beta = \Lambda \quad (1)$

$\vdash . (1) . *11.11.35 . \supset$

$\vdash :: (\exists x, y) . \alpha = \iota'x . \beta = \iota'y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \quad (2)$

$\vdash . (2) . *11.54 . *52.1 . \supset \vdash . \text{Prop}$

AUTOMATH

N.G. de Bruijn:

1967: wiskundige taal **AUTOMATH**

gebruik **computer** om wiskunde volledig formeel te coderen

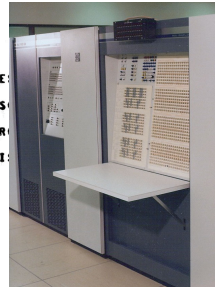
```
U0      := INN(1,U)      : NAT
T1      := 1TOP(1,U)     : LESSIS(U0,1)
T2      := ORE2(MORE(U0,1),IS(U0,1),SATZ24(U0),
              SATZ100(U0,1,T1)) : IS(U0,1)
TM1     := TRIS(1TO(1),U,OUTM(1,U0,T1),10,
              ISOUTINN(1,U),ISOUTNI(1,U0,T1,1,
              LESSIS12(1,1,REFIS(NAT,1)),T2)) : IS"E"(1TO(1),U,10)

-SINGLET

@ 2      := PL(1,1)      : NAT
[X:NAT]

•PAIR

[L:LESSIS(X,2)](N:NIS(X,2))
T1      := SATZ26(1,X,ORE1(LESS(X,2),IS(X,2),L,N)
              ) : LE
T2      := ORE2(MORE(X,1),IS(X,1),SATZ24(X),
              SATZ100(X,1,T1)) : IS
L @ TM1 := TH2"L OR"(IS(X,1),IS(X,2),(T1NIS(X,2))
              T2(T)) : OR
@ TH2   := TH1"E NOTIS"(NAT,<1>SUC,1,2,<1>AX3,
              SATZ4E(1)) : NI
```



een heel wiskundeboek coderen

Grundlagen der Analysis

wiskundeboek van 158 pagina's

volledige nette definitie van

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

plus alle operaties op deze verzamelingen



Edmund Landau
1929

Checking Landau's 'Grundlagen' in the AUTOMATH system

proefschrift

volledig formele versie

ongeveer 10,000 regels AUTOMATH



Bert Jutting
1976

Coq

typentheorie

moderne versie van
AUTOMATH en
formele wiskunde



Gérard
Huet



Thierry
Coquand



Christine
Paulin

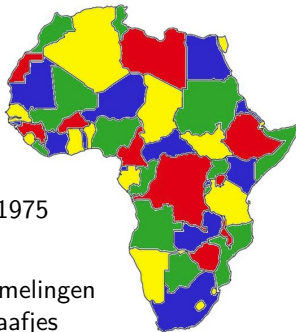
pCIC = predicative **Calculus of Inductive Constructions**

de **Coq** bewijsassistent
INRIA, Frankrijk



de vierkleurenstelling

- ▶ Francis Guthry, 1852
vraag
- ▶ Percy Heawood, 1890
bewijs van **vijfkleurenstelling**
- ▶ Kenneth Appel & Wolfgang Haken, 1975
bewijs van **vierkleurenstelling**
computer berekent gigantische verzamelingen
kleuringen van een hele catalogus graafjes
ingewikkeld computerprogramma
heel lange berekening
computer controleert het bewijs *niet!*
- ▶ Neil Robertson, Daniel Sanders, Paul Seymour, Robin Thomas, 1997
nette versie van bewijs en programma



'mathematical components' project van Microsoft

Coq versie van vierkleurenstelling

- ▶ formele versie van het bewijs
- ▶ programmacorrectheid
Coq als functionele programmeertaal



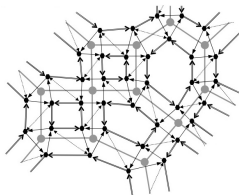
Georges Gonthier
2005

nieuwe technologieën:

- ▶ wiskundige taal **Ssreflect**

Feit-Thompson stelling

- ▶ hypermaps



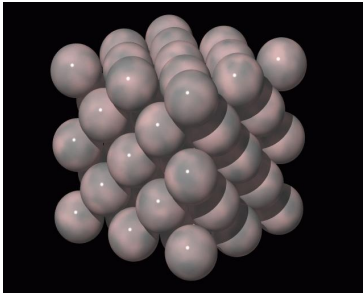
Assia Mahboubi

voorbeeld van een formeel Coq bewijs

```
Lemma no_minSimple_odd_group (gT : minSimpleOddGroupType) : False.
Proof.
have [/forall_inP | [S [T [_ W W1 W2 defW pairST]]]] := FTtypeP_pair_cases gT.
  exact/negP/not_all_FTtype1.
have xdefW: W2 \x W1 = W by rewrite dprodC.
have pairTS := typeP_pair_sym xdefW pairST.
pose p := #|W2|; pose q := #|W1|.
have p'q: q != p.
  have [[ctiW _ _] _ _ _] /mulG_sub[sW1W sW2W]] := (pairST, dprodW defW).
  have [cycW _ _] := ctiW; apply: contraTneq (cycW) => eq_pq.
  rewrite (cyclic_dprod defW) ?(cyclicS _ cycW) // -/q eq_pq.
  by rewrite /coprime gcdnn -trivg_card1; have [] := cycTI_nontrivial ctiW.
without loss{p'q} ltqp: S T W1 W2 defW xdefW pairST pairTS @p @q / q < p.
  move=> IH_ST; rewrite neq_ltn in p'q.
  by case/orP: p'q; [apply: (IH_ST S T) | apply: (IH_ST T S)].
have [[_ maxS maxT] _ _ _] := pairST.
have [[U StypeP] [V TtypeP]] := (typeP_pairW pairST, typeP_pairW pairTS).
have Stype2: FTtype S == 2 := FTtypeP_max_typeII maxS StypeP ltqp.
have Ttype2: FTtype T == 2 := FTtypeP_min_typeII maxS maxT StypeP TtypeP ltqp.
have /mmax_exists[L maxNU_L]: 'N(U) \proper setT.
  have [[_ ntU _ _] cUU _ _ _] := compl_of_typeII maxS StypeP Stype2.
  by rewrite mFT_norm_proper // mFT_sol_proper abelian_sol.
have /mmax_exists[M maxNV_M]: 'N(V) \proper setT.
  have [[_ ntV _ _] cVV _ _ _] := compl_of_typeII maxT TtypeP Ttype2.
  by rewrite mFT_norm_proper // mFT_sol_proper abelian_sol.
have [[maxL sNU_L] [maxM sNV_M]] := (setIdP maxNU_L, setIdP maxNV_M).
have [frobL sUH _] := FTtypeII_support_facts maxS StypeP Stype2 pairST maxNU_L.
have [frobM _ _] := FTtypeII_support_facts maxT TtypeP Ttype2 pairTS maxNV_M.
```

etcetera

vermoeden van Kepler



kubisch-vlakgecentreerde bolstapeling

strena seu de nive sexangula
over de zeshoekige sneeuwvlok



Johannes Kepler
1611



het Flyspeck project

- ▶ 1996: bewijs van het vermoeden van Kepler
boek van 334 pagina's
gigabytes aan data en
dagen aan computerberekeningen
- ▶ reviewers van de *Mathematische Annalen*:
kunnen geen fouten vinden, maar
te ingewikkeld om te controleren



Tom Hales

2003: Flyspeck project =
volledig formele versie van dit bewijs

HOL Light bewijsassistent
(+ Isabelle bewijsassistent)

- ▶ 2014: formele bewijs van het vermoeden van Kepler voltooid
onmogelijk dat er nog ergens een vergissing zit

voorbeeld van een formeel HOL bewijs

$$\begin{aligned} \vec{w} &\neq \vec{0} \wedge \\ \vec{u} \cdot \vec{w} &= \vec{v} \cdot \vec{w} \Rightarrow \\ \angle(\vec{u} \times \vec{w}, \vec{u} \times \vec{w}) &= \angle(\vec{u}, \vec{v}) \end{aligned}$$



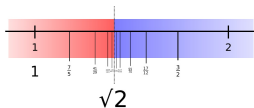
John Harrison

```
let VECTOR_ANGLE_DOUBLECROSS = prove
('!u v w.
  ~(w = vec 0) /\ u dot w = &0 /\ v dot w = &0
  ==> vector_angle (u cross w) (v cross w) = vector_angle u v',
  REPEAT GEN_TAC THEN ASM_CASES_TAC 'u:real^3 = vec 0' THENL
    [ASM_REWRITE_TAC[vector_angle; CROSS_0]; ALL_TAC] THEN
  ASM_CASES_TAC 'v:real^3 = vec 0' THENL
    [ASM_REWRITE_TAC[vector_angle; CROSS_0]; ALL_TAC] THEN
  STRIP_TAC THEN
  SUBGOAL_THEN '~(u cross w = vec 0) /\ ~(v cross w = vec 0)' ASSUME_TAC THENL
    [REPEAT(POP_ASSUM MP_TAC) THEN REWRITE_TAC[GSYM DOT_EQ_0] THEN VEC3_TAC;
     ALL_TAC] THEN
  ASM_SIMP_TAC[VECTOR_ANGLE_EQ] THEN
  SIMP_TAC[vector_norm; GSYM SQR_T_MUL; DOT_POS_LE] THEN
  ASM_REWRITE_TAC[DOT_CROSS; REAL_MUL_LZERO; REAL_SUB_RZERO] THEN
  REWRITE_TAC[REAL_ARITH '(x * y) * (z * y):real = (y * y) * x * z'] THEN
  SIMP_TAC[SQR_T_MUL; DOT_POS_LE; REAL_LE_SQUARE; REAL_LE_MUL] THEN
  SIMP_TAC[SQR_T_POW_2; DOT_POS_LE; GSYM REAL_POW_2] THEN REAL_ARITH_TAC);;
```

Dedekindsneden en Cauchyrijtjes



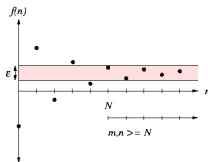
Richard Dedekind



een linker- en een
rechterverzameling



Augustin-Louis Cauchy



equivalentieklasse van
convergerende rijtjes

homotopie-typentheorie

Fields medal 2002

- ▶ homotopietheorie algebraïsche variëteiten
- ▶ formulering van motivische cohomologie



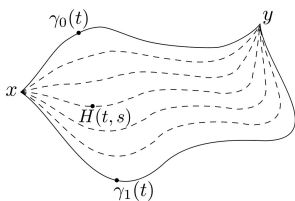
Vladimir Voevodsky
2006

wiskunde onafhankelijk van specifieke definities

homotopie-typentheorie

homotopie als de 'juiste' notie van gelijkheid

homotopie = continue vervorming



twee revoluties

constructieve wiskunde en formele wiskunde

wiskunde versus computers:



‘bewijzen zijn programma’s’



‘programma’s checken bewijzen’

en een puzzel...

een rijtje getallen van N.G. de Bruijn

What is the rule by which the sequence is formed?

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

oplossing (rij A229140 van de OEIS)

1	$1 = 0^2 + 1^2$	0
2	$2 = 1^2 + 1^2$	1
3		
4	$4 = 0^2 + 2^2$	0
5	$5 = 1^2 + 2^2$	1
6		
7		
8	$8 = 2^2 + 2^2$	2
9	$9 = 0^2 + 3^2$	0
10	$10 = 1^2 + 3^2$	1
11		
12		
13	$13 = 2^2 + 3^2$	2
14		
15		
16	$16 = 0^2 + 4^2$	0
17	$17 = 1^2 + 4^2$	1
18	$18 = 3^2 + 3^2$	3
19		
20	$20 = 2^2 + 4^2$	2
21		
22		
23		
24		
25	$25 = 0^2 + 5^2$	0
26	$26 = 1^2 + 5^2$	1
27		
28		