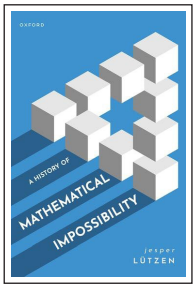
Boekbesprekingen

| Book Reviews

Redactie: Hans Cuypers en Hans Sterk
Secretariaat: Enna van Dijk

Review Editors NAW - MF 5.096a
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
Postbus 513
5600 MB Eindhoven

reviews@nieuwarchief.nl
www.win.tue.nl/wgreview



Jesper Lützen

A History of Mathematical Impossibility

Oxford University Press, 2023
xi + 284 p., prijs £ 28.99
ISBN 9780192867391

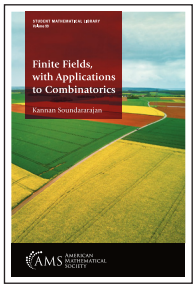
Dit boek biedt een min of meer chronologisch overzicht van wat men wiskundige onmogelijkheid kan noemen, van de oude Grieken tot het heden. Wat er precies met deze onmogelijkheid bedoeld wordt en hoe wiskundigen daar mee omgingen en hoe dat ook veranderde in de tijd, is wat mij betreft de kern van dit zeer leesbare en fraai uitgevoerde (ook nog eens aangenaam geprijsde) boek. Het belang van het rigoureus bewijzen van een wiskundige onmogelijkheid (ik houd die term nog even vaag) werd door wiskundigen pas ingezien in de 17e eeuw. Sowieso zijn wiskundigen altijd meesters geweest in het aanpassen van de regels van het spel (vandaar de introductie van de niet-gehele en later de negatieve, de irrationale en de complexe getallen) en dat maakt dat de wiskunde zich enorm heeft ontwikkeld, altijd gedreven door de gevoelde noodzaak onmogelijkheden op te heffen (“things are only impossible until they are not”), maar soms alleen maar vanwege de hoop van soms zeer fanatieke amateurs op eeuwige roem of op een som geld en/of omdat men eenvoudigweg niet goed begreep welke claim werd uitgesproken en wat men precies moest aantonen of oplossen. Vele bekende zaken (de kwadratuur van de cirkel, de verdubbeling van de kubus, de trisectie van een hoek, al dan niet met passer en ongemarkeerde liniaal te construeren veelhoeken, de bruggen van Königsberg, de niet-Euclidische meetkunde, het vermoeden van Fermat c.q. de stelling van Wiles, de irrationaliteit en de transcendentie van π en e, het oplossen van vijfde- en hogeregraadsvergelijkingen, de onvolledigheidsstellingen van Gödel en nog veel meer) passeren de revue, maar omdat elke groeispurt van de wiskunde weer leidde tot nieuwe en preciezere inzichten en dus ook tot nieuwe pogingen (nog meer) grip te krijgen op eerder onmogelijk geachte zaken, komen deze in dit boek dus meerdere malen (en vaak zeer uitvoerig) aan de orde en dat is zeer verhelderend.

Zo wordt bijvoorbeeld uitgelegd dat in de 17e eeuw de klassieke constructieproblemen nauwelijks werden bestudeerd, omdat men dacht dat de door Descartes ontwikkelde analytisch meetkundige aanpak wel de oplossingen voor die problemen zouden onthullen. En ook dat de in 1768 bewezen irrationaliteit van π de grootste 18e-eeuwse bijdrage was aan het uiteindelijke bewijs van de onmogelijkheid van de kwadratuur van een cirkel (pas in 1882 bewezen, grotendeels gebaseerd op de in datzelfde jaar bewezen transcendentie van π). Het voor elke brugklasser geen geheimen kennende minteken werd (samen met het wortelteken) pas rond 1550 door Cardano geïntroduceerd bij zijn pogingen tweedegraadsvergelijkingen algemener dan daarvoor op te lossen en het is immer weer boeiend om te lezen hoe daarna het zelfs accepteren van wortels van negatieve getallen ervoor zorgde dat men reële oplossingen van derdegraadsvergelijkingen kon vinden (prachtig verwoord met “the unreasonable usefulness of the complex numbers”, het sterkste voorbeeld van een theorie die slechts om puur wiskundige

redenen was bedacht en later essentieel bleek in wiskundige en fysische toepassingen). Snel (ook in 1882, Abel) volgde wellicht het eerste echte voorbeeld van de nadruk die werd gelegd op en het belang dat werd gehecht aan het bewijzen van een onmogelijkheid, namelijk die van het – in dit geval – vinden van formules om vergelijkingen op te lossen van graad 5 en hoger, in plaats van te blijven proberen zulke formules te vinden. Even later gevolgd door het vinden van voorwaarden om een vergelijking wel algebraïsch op te kunnen oplossen, resulterend in de Galois-groepentheorie en de geboorte van de moderne algebra. De daaruit ontstane nieuwe algebraïsche methoden bleken zeer geschikt om uiteindelijk allerlei onmogelijkheden te bewijzen of eerdere bewijzen daarvan overtuigender te maken.

Van puur meetkundige aard zijn de uitvoerig beschreven pogingen het vijfde (parallellen)postulaat van Euclides te bewijzen en de later gebleken onmogelijkheid daarvan (en de daaruit voortvloeiende keuze om de niet-Euclidische meetkunde te ontwikkelen, die van groot belang bleek te zijn voor de hedendaagse, moderne natuurkunde en ook zeer toepasbaar op de fysieke wereld waarin we leven). In deze bespreking mag uiteraard de grote Duitse wiskundige Hilbert niet ontbreken, die in 1900 zijn fameuze lezing hield waarin hij slechts tijd had om 10 (van zijn lijst van 23) problemen te formuleren. Hilbert was min of meer van mening dat elk correct gesteld probleem bewijsbaar zou moeten zijn (“for in mathematics there is no ignorabimus”) en verder dat zonder het formuleren van problemen de ontwikkeling van de wiskunde stil zou vallen. Een van die problemen (het derde) werd binnen een jaar opgelost en wel door te bewijzen dat het niet altijd mogelijk was twee veelvlakken met hetzelfde volume te verdelen in dezelfde eindige verzameling viervlakken (analoog aan het wel altijd kunnen verdelen van twee verschillende veelhoeken met gelijke oppervlakte in dezelfde eindige verzameling driehoeken). Hilberts eerste probleem (de continuümhypothese) bleek onbeslisbaar en had paradoxale gevolgen. De mede hierdoor verder ontwikkelde verzamelingenleer (Cantor, Zermelo) was pas veel later (in 1940, Gödel en in 1963, Cohen) in staat hier meer substantieels over te zeggen. De zojuist al genoemde Gödel had al eerder (in 1931) een enorme bom gegooid in de toch al niet rimpelloze vijver die wiskunde heet en daarmee bleek de hoop die Hilbert koesterde op een formele axiomatisatie van elke tak van wiskunde ijdel. Maar (zo stelt Lützen), Gödels resultaten kunnen ook worden opgevat als oplossingen van de gestelde problemen en ze demonstreren juist de kracht van de wiskunde, in het bijzonder om haar grenzen te verkennen. Hilbert had weliswaar het vermoeden van Fermat ($x^n + y^n = z^n$ met gehele en positieve x, y en z en voor $n \geq 3$ heeft geen oplossingen) niet op zijn lijst staan, maar hij voorspelde correct dat het – naar later bleek zeer ingewikkelde – bewijs zou worden geleverd in de 20e eeuw, zodat zijn optimisme niet helemaal vreemd was.

Aan het einde van het boek nog een uitstapje naar Arrow’s Impossibility Theorem (over verkiezingen en stemgedrag en de daarbij voorkomende paradoxen) en de natuurkunde (vanwege de vele wiskundige wetmatigheden die de realiteit beschrijven en kunnen duiden). De genoemde (on)mogelijkheden (quantummechanica, perpetuum mobile, big bang, reizen door de tijd) laat ik aan de lezer. Een zeer secuur en helder geschreven en mooi opgebouwd boek (niveau 6 vwo, eerstejaars bètastudie) dat ik van harte kan aanbevelen. *Joop van der Vaart*



Kannan Soundararajan

Finite Fields, with Applications to Combinatorics

Student Mathematical Library Volume 99

AMS, 2022
170 p., prijs $ 47.20
ISBN 9781470469306

Finite fields are a mathematical topic mostly introduced in the later years of a bachelor program. The author of this book attempts to not only introduce this topic to first year students, but also to provide a number of fun applications in combinatorics, and to show how they are used in the AKS Primality Test, the first algorithm that can provably determine whether or not a given positive integer is a prime number in polynomial time. The prerequisites are familiarity with proof writing, linear algebra, and one variable calculus. The book is of interest to undergraduate students who want to learn about some basic algebra, number theory, and finite fields (the first six chapters and Chapter 9), as well as to those with some knowledge of finite fields who are interested in applications (Chapter 7 for combinatorics, Chapter 8 for AKS). As an educator, I found that the first chapter might be the most challenging for students, as it covers various algebraic topics in very little detail. The remaining chapters cover much less new material, and many take the time to cover just the little bit of material required for the rest of the chapter. Each chapter has a number of exercises that seem suitable for students. As a mathematician, I appreciated chapters 7 and 8 the most, since I was not familiar with the topics (I knew of the existence of the AKS Primality Test, but not much more). These chapters were written on a level that I think can be understood by a student, with some exercises covering the more technical parts of the proof. I would say that all the basics on finite fields are covered, maybe with the exception of the automorphism group and the Frobenius automorphism (the latter of which is seen in an exercise, but not mentioned by name), and various related topics are covered as a consequence. The book is not a full substitute for an algebra course; many topics you expect from an algebra course are covered throughout the book, but some are skipped. As an example, isomorphisms of groups and rings are covered (to the extent of explaining what is meant by groups and rings being isomorphic), but homomorphisms are not.

Some more detail on each chapter can be found below.

Chapter 1 mainly covers basic algebra. It starts by briefly introducing groups, rings, domains and fields, and follows up by introducing primes and irreducibles in an integral domain, ideals and principal ideal domains, Euclidean domains, and the topic of unique factorization. As mentioned, this chapter is very sparse on details. Fortunately, one doesn’t need more than the definitions and some basic examples for the rest of the book.

Chapter 2 is more number-theoretic in nature, covering the infinitude of primes, Bertrand’s postulate that for every natural number $n \geq 1$ there is a prime p with $n + 1 \leq p \leq 2n$, both proven in the text. It also covers – without proof – the prime number theorem, which one can use to estimate the number of primes less than x.

Chapter 3 introduces quotient rings, integers modulo n, prime

and maximal ideals, and primes in the Gaussian integers.

Chapter 4 covers primes in the polynomial ring over $\mathbb{Z}/p\mathbb{Z}$ with p a prime, showing existence of finite fields of order p^n for all positive integers n, and giving an analogue to Bertrand's postulate and to Euler's proof of the infinitude of primes, ending with Möbius inversion to count the number of monic irreducible polynomials of degree n, as well as to find $\phi(n)$, the number of invertible elements modulo n.

Chapter 5 covers cyclic groups, Lagrange's Theorem on the order of subgroups, and applies these to give the additive and multiplicative structure of all finite fields.

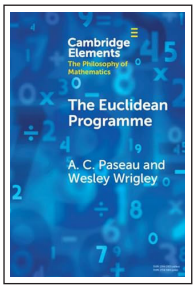
Chapter 6 is on number theory again; it covers the Chinese Remainder Theorem for $\mathbb{Z}/n\mathbb{Z}$, the structure of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ and the existence of primitive roots modulo p^e for odd primes p.

Chapter 7 contains two main parts. One is on Sidon sets, finite sets of integers $\{a_1, a_2, \ldots, a_k\}$ such that the sums $a_i + a_j$ with $1 \leq i \leq j \leq k$ are all distinct. Some bounds on the sizes of such sets as shown, and finite fields are used to construct Sidon sets of large size. The second part is on De Bruijn sequences, cyclic strings S of n^l letters in an alphabet of size n such that every string of l letters occurs exactly once as a substring of S. An application of finite fields shows that for all positive integers l, De Bruijn sequences of size n^l exist if n is a prime power.

Chapter 8 goes into detail about the AKS primality test.

Chapter 9 summarizes the material on finite fields, and additionally shows that all finite fields of size p^k are isomorphic and classifies the subfields of the finite field of size p^k.

Rob Eggermont



A.C. Paseau, Wesley Wrigley

The Euclidean Programme

Cambridge Elements: The Philosophy of Mathematics

Cambridge University Press, 2024
ii + 74 p., prijs € 19,84
ISBN 9781009221986

In 1962 R.L. Goodstein and I. Lakatos published a paper called *The Foundations of Mathematics* in *Aristotelian Society Supplementary Volume* (Volume 36, Issue 1, 15 July 1962, Pages 145–184). It would be more accurate to say that it is the union of two papers: Goodstein discusses *The Axiomatic Method*, and Lakatos' part is called *Infinite Regress and the Foundations of Mathematics*. It is the latter part that serves as the main inspiration for the book(let) under review. In it, Lakatos described the infinite regress that invariably appears when we try to define the mathematical notions that occupy us. No definition is truly definitive: every definition contains a reference to another notion, or a synonym. Euclid's definition of 'point' contains the undefined notion 'breadth'; Cantor's definition of 'Menge' contains the synonym 'Zusammenfassung'. In the paper Lakatos deals with three programmes that attempt to fix the foundations once and for all: (1) the Euclidean programme (2) the Empiricist programme and (3) the Inductivist programme.

In short: a Euclidean starts at the top with propositions (*axioms*) that contain perfectly well-known terms (*primitive terms*) and if there are (infallible) truth assignments that make them *True*, then that truth flows down to other propositions via suitable deductions and will permeate the whole system.

An Empiricist starts at the bottom with propositions (*basic statements*) that contain perfectly well-known terms (*empirical terms*) and if it is possible to (infallibly) assign the truth-value *False* to some then that value flows up to higher propositions (*explanations*) and will infect all these explanations.

Usually *True* does not flow up: implications do not always reverse. An Inductivist tries to find a way through which truth flows up anyway. Sherlock Holmes was an inductivist who used abduction rather than deduction to find the most probable explanation for the observed phenomena.

Lakatos described how even in the beginning of the 20th century people strove to lay Euclidean foundations for mathematics, but that each attempt furnished another step in the infinite regress described above. The combined paper is well worth reading and it puts very much paid to the aspirations of the Euclidean programme.

So what does the present work have to offer?

For starters a more formal description of what the/a Euclidean programme (abbreviated as EP by the authors) should look like. First there is a ternary (epistemic) relation $E(S,p,d)$ read as "the subject S is related to the proposition p to a degree d". The relation can be: 'grasping' (understanding what it says), 'believing' (based on observation or on proof), 'knowing', etc. This is left deliberately vague because it may change from case to case.

Next there are three plus four principles of the EP. The first three are the core; they are called EP-Truth, EP-Self-Evidence, and EP-Flow. These state, respectively, that: 1) the axioms and theorems should be true; 2) they should be self-evident, that is, graspable and, once grasped by S, the degree d in $E(S,p,d)$ is maximal; 3) if q follows from some premises $p_1, \cdots, p_n$, then $E(S,q,e)$ holds with a value e equal to or close to the values d_i in the various $E(S,p_i,d_i)$.

Then there are four supplementary/non-core principles: EP-finite, EP-general, EP-independence, and EP-Completeness. Of these, EP-finite and EP-independence are self-explanatory. EP-General wants the axioms to be general statements; though this is deemed standard, the authors also assert that defining 'generality' is hard. A good approximation would be "closed formulas", that is, formulas where all variables are quantified. The most troublesome is EP-Completeness; Gödel's incompleteness theorems make full-fledged completeness – each formula is derivable or its negation is – impossible for most useful theories. The solution here is to lower expectations and expect that at least truths that were known/observed before the axiomatization will be derivable.

The first three more or less formalize Lakatos' looser description, which does not explicitly contain the other four.

In the bulk of the book the authors test four works against the Euclidean Programme, and conversely the Programme itself against modern theories.

The four works are Euclid's *Elements*, Aristotle's *Posterior Analytics*, Descartes' *Discourse de la Methode*, and Pascal's *De l'esprit géométrique et de l'art de persuader*. The first two because they have, through their centuries-long influence, inspired the programme, and the second two because they are deemed to symbolize, or be part of, the apogee of the programme.

Maybe surprisingly, the authors find that Euclid in his *Elements* does not really adhere to the Euclidean Programme. I write "not really", because the arguments are largely indirect: The *Elements* makes no statements as to the truth or self-evidence of the axioms and theorems, nor of the way truth is supposed to flow through the work. We can only observe, and with modern eyes we see that all three core principles are absent. The Parallel Postulate was never self-evident, given the many attempts to prove it, and it fails in the hyperbolic plane. The very first proof contains a gap, so truth does not flow through it.

Aristotle's work specifies the nature of the axioms and of deductions/derivations quite explicitly, but here the Euclidean Programme is in the eye of the reader. EP-Truth and EP-Self-Evidence may or may not hold, depending on interpretation, EP-Flow does hold.

Descartes and Pascal pass the EP-exam, at least with respect to the three core principles. These appear more or less explicitly in their explanations.

These last three authors get mixed marks on the four other principles. Often because there is no explicit mention. Aristotle may be read to desire Generality and Independence, and Descartes and Pascal indicate a desire for completeness, but there are no really definite pronouncements.

In the opposite direction the authors test the EP against present-day mathematics, represented here by Set Theory, (Peano) Arithmetic, and Group Theory. All three adhere to EP-Truth. Arithmetic somewhat more naturally than the others: Peano's Axioms hold in the intended interpretation: *the* natural numbers. The Set-Theoretic axioms were formulated to describe the workings of sets in such a way that the known paradoxes would be avoided. The group axioms simply tell us what a group is. One could say that the latter two have axioms that are true by stipulation. This makes the case for EP-Self-Evidence somewhat problematic. Apart from the Induction scheme the Peano axioms are quite self-evident, because we have seen them happen often enough. If the Induction scheme is applied to a very large formula, however, then that particular instance may no longer be graspable and hence not self-evident. The axioms for Set Theory are graspable, but they lay no claim to self-evidence and they were not intended to be; they should protect us from paradoxes and make work in Set Theory possible (this is my paraphrasing). The Group Axioms are graspable. Are they self-evident? Maybe, maybe not, but they do the work.

According to the authors we have lost EP-Flow, not because of the rules of deductions, but because we are only human: if the proof of q from p is (veeery) long (the abc-conjecture, for example…), the e in $E(S,q,e)$ may be a lot smaller than the d in $E(S,p,d)$.

Of the four subsidiary principles EP-General holds: all axioms are closed formulas. One can argue that EP-Finite holds as well, certainly for groups, and if one treats an axiom scheme such as Induction as one template, it also holds for the other two theories.

There is a certain redundancy in the axioms for Set Theory and Arithmetic. In Set Theory one can dispense with the Separation Scheme and prove all instances from the Replacement Scheme, assuming the latter is formulated appropriately, and in Arithmetic some instances of Induction can be used to prove others. The group axioms are independent. So EP-Independence is not something that we always strive for.

EP-Completeness is hard to come by thanks to Gödel's incompleteness theorems. This theorem does not apply to group theory, but the axioms are incomplete anyway: they prove neither $(\forall x)(\forall y)(x*y=y*x)$ nor its negation.

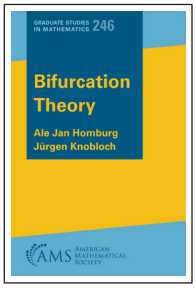
To summarize: modern mathematics has given up basically all principles, except maybe EP-truth, but only because we simply stipulate that the axioms are true.

So, what to make of this book? I see it mostly as an intellectual exercise: there is this thing called *Euclidean Programme*, let us investigate whether this can be found in the wild. The last chapter looks at what the alternatives are, if any. I write "if any" because from what I have seen of the work on the foundations of mathematics, I get the idea that the true foundations are just around the corner, where Lakatos' infinite regress shows a long queue of candidates waiting to claim to be the real thing. Nevertheless the authors have a few pointers, illustrated by a quote from Gödel who advocates looking at the 'success' of an axiom system or just a single axiom: how it illuminates or explains more things in a better way. This looks like a version of the Empiricist's programme: not quite looking to falsify, but looking for analogies in the spirit of this quote, attributed to Banach: "Good mathematicians see analogies between theorems or theories, the very best ones see analogies between analogies."

I myself like how Bottema, in his lecture *Euclides in Wonderland*, tested mathematics against Huizinga's definition of a game: *A voluntary act or activity, that is performed within certain determined limits of time and place, according to voluntarily accepted, yet strictly binding rule(s), with its purpose in itself, accompanied by a feeling of excitement and joy, and by the realization of "being different" from daily life* (een vrijwillige handeling of bezigheid, die binnen zekere vastgestelde grenzen van tijd en plaats wordt verricht, naar vrijwillig aanvaarde, doch volstrekt bindende regel, met haar doel in zichzelf, begeleid door een gevoel van spanning en vreugde, en door een besef van "anders zijn" dan het gewone leven; *Euclides*, **25** (III), 98–117 (1951/52)). Mathematics passes with flying colours.

K.P. Hart

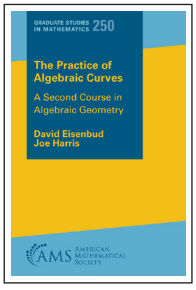
Recent verschenen publicaties. Als u een van deze boeken wilt bespreken of als u suggesties heeft voor andere boeken voor deze rubriek, laat dit dan per e-mail weten aan reviews@nieuwarchief.nl.



Ale Jan Homburg, Jürgen Knobloch

Bifurcation Theory

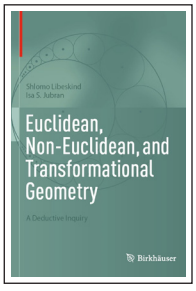
AMS, 2024
ISBN 9781470478803
https://bookstore.ams.org/view?ProductCode=GSM/246



David Eisenbud, Joe Harris

The Practice of Algebraic Curves
A Second Course in Algebraic Geometry

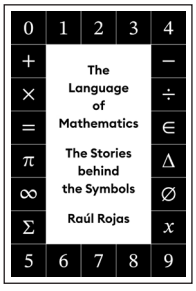
AMS, 2024
ISBN 9781470479435
https://bookstore.ams.org/view?ProductCode=GSM/250



Shlomo Libeskind, Isa S. Jubran

Euclidean, Non-Euclidean, and Transformational Geometry. A Deductive Inquiry

Springer (Birkhäuser), 2024
ISBN 9783031741524
https://link.springer.com/book/10.1007/978-3-031-74153-1



Raúl Rojas

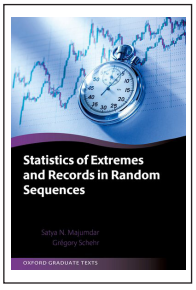
The Language of Mathematics
The Stories behind the Symbols

Princeton University Press 2025
ISBN 9780691201887
https://press.princeton.edu/books/hardcover/9780691201887/the-language-of-mathematics

Roel Andringa-Boxum

Schitterende Symmetrieën
De Natuurwetten in een Handomdraai

Epsilon Uitgaven 2024
ISBN 9789050412087
https://www.epsilon-uitgaven.nl/wetenschappelijke-reeks/schitterende-symmetrieen/11204



Satya N. Majumdar, Grégory Schehr

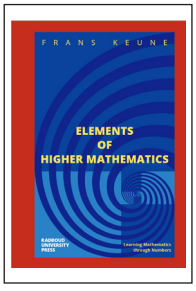
Statistics of Extremes and Records in Random Sequences

OUP 2024
ISBN 9780198797333
https://global.oup.com/academic/product/statistics-of-extremes-and-records-in-random-sequences-9780198797333

Peter D. Schumer

Fractions. A Sliver of the Story

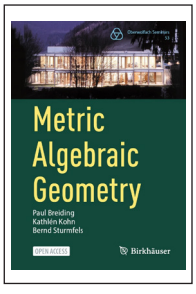
Open University Press 2024
ISBN 9780198916536
https://global.oup.com/academic/product/fractions-9780198916536



Frans Keune

Elements of Higher Mathematics

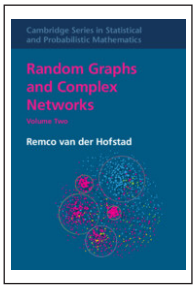
Radboud University Press 2024
ISBN 9789493296824
https://books.radbouduniversitypress.nl/index.php/rup/catalog/book/elements_of_higher_mathematics



Paul Breiding, Kathlén Kohn, Bernd Sturmfels

Metric Algebraic Geometry

Springer 2024
ISBN 9783031514616
https://link.springer.com/book/10.1007/978-3-031-51462-3



Remco van der Hofstad

Random Graphs and Complex Networks, Volume 2

Cambridge University Press 2024
ISBN 9781107174009
https://www.cambridge.org/nl/universitypress/subjects/statistics-probability/applied-probability-and-stochastic-networks/random-graphs-and-complex-networks-volume-2