Dierk Schleicher • Malte Lackmann
Editors

An Invitation to Mathematics

From Competitions to Research

Springer

Editors
Dierk Schleicher
Jacobs University
Postfach 750 561
D-28725 Bremen
Germany
dierk@jacobs-university.de

Malte Lackmann
Immenkorv 13
24582 Bordesholm
Germany
malte.lackmann@web.de

ISBN 978-3-642-19532-7 e-ISBN 978-3-642-19533-4
DOI 10.1007/978-3-642-19533-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011928905

Mathematics Subject Classification (2010): 00-01, 00A09, 00A05

Cover design: deblik, Berlin

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Contents

Preface: What is Mathematics?

Günter M. Ziegler

This book is an Invitation to Mathematics.

But *What is Mathematics*? This is a question that asks us for a definition. You could look in *Wikipedia* and find the following:

> *Mathematics is the study of quantity, structure, space, and change. Mathematicians seek out patterns, formulate new conjectures, and establish truth by rigorous deduction from appropriately chosen axioms and definitions.*

Quantity, structure, space, and change? These words outline a vast field of knowledge — and they are combined with a very narrow, mechanistic, and, frankly, quite boring description of "what mathematicians do". Should "what mathematicians do" really be a part of the definition?

The definition given by the German *Wikipedia* is interesting in a different way: it stresses that there is no definition of mathematics, or at least no commonly accepted one. I translate:

> *Mathematics is the science that developed from the investigation of figures and computing with numbers. For mathematics, there is no commonly accepted definition; today it is usually described as a science that investigates abstract structures that it created itself for their properties and patterns.*

Is this a good definition, a satisfactory answer to the question "What is Mathematics"? I believe that *Wikipedia* (in any language) does not give a satisfactory answer. At the same time, and much more importantly, high school curricula do not give a satisfactory answer. Even the famous book by Richard Courant and Herbert Robbins entitled "What is Mathematics?" (and subtitled "An Elementary Approach to Ideas and Methods") does not give a satisfactory answer.

Günter M. Ziegler
Fachbereich Mathematik und Informatik, Freie Universität Berlin, Arnimallee 2, 14195 Berlin, Germany. e-mail: ziegler@math.fu-berlin.de

Perhaps it is impossible to give a good definition in a sentence or two. Indeed, I claim that there cannot be one single answer that we could be content with: mathematics in the 21-st century is a huge body of knowledge and a very diverse area of study. There are thus so many ways to experience mathematics — the arenas of national and international competitions, and research experiences that range from years spent working in solitude (think of Andrew Wiles, who proved Fermat's Last Theorem, or Grigori Perelman, who proved the Poincaré conjecture) to coffee break discussions at conferences to massive collaborations on internet platforms (such as the POLYMATH projects initiated by Michael Nielsen, Timothy Gowers, Terence Tao, and others).

But perhaps the English *Wikipedia* is right in one aspect — that in approaching the science called mathematics one should look at the people who do mathematics. So *what is mathematics as an experience*? What does it mean to *do* mathematics?

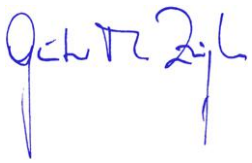
This book is an invitation to mathematics comprised of contributions by leading mathematicians. Many of them were initiated to mathematics, and led to mathematics research, through competitions such as the mathematical olympiads — one of the ways to get attracted to and drawn into mathematics. This book builds a link between the "domesticated" mathematics taught at high schools or used in competitions and the "wild" and "free" world of mathematical research. As a former high school student, successful participant at competitions such as the IMO 1981, and now professor of mathematics who is doing research and who is active in communicating mathematics to the public, I have personally experienced all these kinds of mathematics, and I am excited about this book and the link that it provides.

The starting point of this book was an event that I had the pleasure of hosting (jointly with Martin Grötschel), namely the 50-th International Mathematical Olympiad, held in Bremen in 2009, at which several premier IMO gold medal winners got on stage to talk about the mathematics that they studied, the mathematics that they are studying, and the mathematics that they are interested in.

All this is reflected in this volume, which contains some of these IMO presentations, as well as other facets of the mathematics research experience. It was put together with admirable care, energy, and attention to detail by Dierk Schleicher (one of the chief organizers of the 50-th IMO in Bremen) and Malte Lackmann (a successful three-time IMO participant). Let me express my gratitude to both of them for this volume, which I see as a book-length exposition of an answer to the question "What is Mathematics?" — and let me wish you an informative, enjoyable, and (in the proper sense of the word) *attractive* reading experience.

Berlin, November 2010

Günter M. Ziegler



Welcome!

Dear Readers,

we are pleased that you have accepted our *Invitation to Mathematics*. This is a joint invitation by a number of leading international mathematicians, together with us, the editors. This book contains fourteen individual invitations, written by different people in different styles, but all of us, authors and editors alike, have one thing in common: we have a passion for mathematics, we enjoy being mathematicians, and we would like to share that enjoyment with you, our readers.

Whom is this book written for? Broadly speaking, this book is written for anyone with an interest in mathematics — yes, for people just like you. More specifically, we have in mind young students at high schools or universities who know mathematics through their classes and possibly through mathematics competitions that they have participated in, either on a local level or all the way up to the level of international olympiads. Mathematics has different flavors: the kind of mathematics found at high school is distinctly different from that found at competitions and olympiads, and both are quite different from mathematics at the research level. Of course, there are similarities too — after all, it's all mathematics we're talking about.

The idea of this book is to allow professional research mathematicians to share their experience and some aspects of their mathematical thinking with our readers. We made a serious effort to reach out to you and write at a level that, for the most part, should be accessible to talented and, most importantly, interested young students in their final years of high school and beyond. Quite importantly, this book is also meant to address high school math teachers, in the hope that they find our invitation interesting as well and share this interest with their students. And of course, we hope that even active research mathematicians will find this book inspiring and, in reading it, will gain new insights into areas outside of their specialization — just as we learned quite a bit of mathematics ourselves in the process of editing this book.

Fourteen invitations to mathematics. You will find that the individual invitations in this book are as varied as the personalities of their authors and their mathematical tastes and preferences: mathematics is a place for very different people. All of our fourteen invitations are independent from each other, and you are welcome to browse through them and start with those that you like best, or that you find most accessible, and continue in your preferred order — much as the white "random path" on the book cover that connects the pictures from the different contributions. (We ordered the contributions by attempting to bring together those that discuss related topics, but of course there would have been many equally good ways to order them.) If you get stuck at one particular invitation, you may want to continue with another. You may discover, though, that some of those that you found difficult at first may become easier, and perhaps more beautiful, once you've learned some more mathematics, or gotten more experience with other invitations, or simply had some time to digest them. Indeed, a number of our contributions are invitations to active reading, and ask you to think along seriously: after all, thinking is what most of us do for much of our professional research time.

Although we encourage you to start by reading those invitations that you prefer, we would like to equally strongly encourage you to fully use the opportunity that this book provides, with the broad area of mathematics that it covers. In high school or during competitions and olympiads, you may have developed preferences for some areas of mathematics or dislikes for others; but mathematics is a broad and rich field, and it is dangerous to become specialized too early, before having seen the beauty of many other mathematical areas. We have often spoken to young university students who thought they were sure they wanted to work in area X and thus refused to take courses in other areas, and advised them to get at least some background in areas Y and Z. Often enough, it turned out that these areas weren't so bad after all, and the students ended up doing their research in areas Y′ or Z′, or possibly Ω. And even for those few who, after having explored different branches of mathematics, ended up working in exactly the area X that they liked best as a young student, it can only be good to take along as many ideas from other areas of mathematics as possible. In modern mathematics, there is increasingly more interaction between different branches that seemed to be drifting apart some time ago. This can be seen quite well in the articles of our book: many contributions cover (apparently) quite different aspects of mathematical research and show surprising links between them. In addition, there are many links between the different contributions, so that you will often have the feeling of meeting similar ideas in quite different contexts. Rather than telling you where, we encourage you to read and discover this on your own.

To paraphrase the spirit of the book, the title is *not* "Fourteen invitations to mathematics", but "An invitation to mathematics", and we hope that you can get a glimpse of mathematics that has as much breadth and variety as we managed to fit between the covers of this book. (Mathematics itself is much broader, of course, and we thought of many further contributions.

If you feel that an important aspect of mathematics is missing here, and that we overlooked a particular person that should have contributed another invitation to mathematics, then please let us know — and help us convince this person to share this invitation with us for the next edition of this book!)

The inspiration for this book. This book was inspired by the 50-th International Mathematical Olympiad that took place in 2009 in Bremen, Germany. Both of us were quite involved in this olympiad: one as a senior organizer, the other as a participant.

One highlight of this olympiad was the 50-th IMO anniversary celebration ceremony, to which six of the world's leading international research mathematicians were invited, all of whom had personal experience with the IMO: Béla Bollobás, Timothy Gowers, László Lovász, Stanislav Smirnov, Terence Tao, and Jean-Christophe Yoccoz. *All six accepted our invitations!* They gave wonderful presentations and were celebrated by the IMO contestants and delegates like movie stars. We tried to provide ample opportunity for IMO contestants and delegates to get in contact with our guests of honor and to have a chance to interact personally with them. This was a most memorable and exciting event that created lasting memories for all of us. We hope that this spirit of personal interaction and invitation will also shine through in this book and its individual contributions.

In addition to the contributions of these guests of honor, three more of our invitations have their roots at the IMO 2009: over the course of three evenings, while the solutions of the contestants were being evaluated, we offered mathematics talks to them (given by Michael Stoll, Marcel Oliver, and Dierk Schleicher). Another contribution (by Alexander Razborov) is based on a lecture series given at the "Summer School on Contemporary Mathematics" held in Dubna/Moscow in 2009. Whatever their inspirations, all contributions were written specifically for this occasion (earlier versions of the contributions by Bollobás, Gowers, Lovász, Smirnov, Tao, and Yoccoz appeared in the report of the 50-th IMO).

This book goes far beyond a single event, exciting as it was, and tries to build lasting links between high schools, competitions, and mathematical research. To use a metaphor of József Pelikán, chairman of the IMO advisory board, research mathematics is like wildlife in uncharted territory, whereas olympiad problems are like animals in a zoo: even though they are presented as animals from the wild, they are constrained to a very restrictive cage. No lion can show its full splendor and strength in the few square meters enclosed by its cage, just as mathematics cannot show its full beauty within the rigid boundaries of competition rules. For young students who have been successful at olympiads, it is important that they learn to leave the olympiad microcosm, to get used to dealing with real mathematical wildlife, and to accept new challenges.

Advertising mathematics, or being a mathematician. We thought about using this introduction to advertise mathematics, including a recitation of the usual

claims about how important mathematics is and how much our culture is built upon mathematical thinking. However, we believe that our readers do not need to be convinced, and that the invitations speak for the beauty and value of mathematics by themselves. Nevertheless, we are aware that many students have parents or counselors who tell them that they should study something that will one day earn them money or that has safer job prospects. To them, we would like to say that young people will be most successful in areas that they enjoy the most, because it is only there that they can develop their full potential. Parents[1], please don't worry: all the students from various countries who wanted to become mathematicians and that we advised to pursue their goals despite the concerns of their parents have become quite successful in their fields, in academia, in industry, or in business, and none of them went unemployed.

What makes this book special. First and foremost, our authors include some of the world's leading mathematicians, who are sharing some of their mathematics with you, our readers. This book wants to build a bridge between active research mathematicians and young students; it was realized by a team of people that come from both ends of this bridge: authors, editors, and test readers.

Indeed, we have not made it easy for our authors to write their contributions: we adopted an editing style that Timothy Gowers, in the preface to his *Princeton Companion to Mathematics*, describes as "active interventionist editing". All contributions have been carefully read by us and by a team of young test readers at the age of the intended readership, and we or the authors improved whatever our team could not understand, until things became clear. In this way, we hope that contributions that were *meant to be* comprehensible to our readers actually *are*: the only way to find out was by asking a number of test readers, and that's what we did.

This resulted in numerous and substantial requests for changes in most contributions. All authors accepted these requests, and many were extremely pleased with the feedback they received from us. One author, who was initially somewhat skeptical about this process, wrote "I am extremely impressed by the quality of the job they have done — it greatly surpasses the average level of referee reports I have seen in all three major capacities (editor, author or, well, referee)". In the preface to his *Princeton Companion*, Timothy Gowers writes "given that interventionist editing of this type is rare in mathematics, I do not see how the book can fail to be unusual in a good way". With due modesty, we hope that this applies to some extent to this book as well, and

[1] Additional evidence for parents: just a year ago, the *Wall Street Journal* published a ranking of 200 jobs according to five important criteria: work environment, income, employment outlook, physical demands, and stress. The jobs investigated included such different occupations as computer programmer, motion picture editor, physicist, astronomer, and lumber jack. What are the top three jobs? In order, they are: mathematician, actuary, and statistician. All three jobs are based on a strong mathematics education. (Source: http://online.wsj.com/article/SB123119236117055127.html.)

that our readers will appreciate the outcome of the substantial efforts of our authors and our editorial team — our test readers, at least, told us many times that they did.

We would like to conclude this *Welcome* with quotations from two more of our test readers: "I never thought that the topic XY could be exciting to read; well, now I know, it can be!" Another one wrote, after reading a different contribution: "I really found this text very interesting to read; and this really means something because this is not an area I thought I was interested in!"

This is the spirit in which we would like to encourage you to read this book.

Bremen, November 2010

Malte Lackmann and Dierk Schleicher

Acknowledgements. First and foremost, we are indebted to the authors of our *Invitation to Mathematics*. Their willingness to provide their contributions and to share their personal insights, as well as their positive attitude with which they responded to our numerous requests for improvements, are greatly appreciated by us and, we hope, also by our readers. We had a number of "test readers" from the target group of students who patiently and carefully read through some or even all of the invitations, sometimes in several versions, and who helped the authors and us produce a much better book. Several of our authors specifically asked us to convey their appreciation to our test readers for their dedication and care, and we do this with great happiness and gratitude. Our most active test readers were Alexander Thomas, Bertram Arnold, and Kęstutis Česnavičius, but many more students read one or several texts and gave us valuable feedback, including Bastian Laubner, Christoph Kröner, Dima Dudko, Florian Tran, Jens Reinhold, Lisa Sauermann, Matthias Görner, Michael Meyer, Nikita Selinger, Philipp Meerkamp, and Radoslav Zlatev, as well as our colleagues and friends Marcel Oliver and Michael Stoll. We would also like to thank Jan Cannizzo, who greatly helped us take care of English language issues in the texts, and who language edited several contributions entirely; our authors specifically asked us to thank him sincerely. We are extremely grateful to Clemens Heine from Springer Verlag for his untiring and continuous factual and moral support in all kinds of circumstances; if it is ever true to say that a book would not have come into existence without the continuous support of the publishing editor, it is the case here. It has also been a pleasure to work with Frank Holzwarth from Springer Verlag who solved all our LaTeX issues in an instant.

We gratefully acknowledge advice and suggestions shared with us by many colleagues, including Béla Bollobás, Timothy Gowers, Martin Grötschel, and most importantly Günter Ziegler. We would like to thank all those who made the IMO 2009 a success and an inspiration, first and foremost our friends and colleagues in the IMO 2009 steering committee: Anke Allner, Hans-Dietrich Gronau, Hanns-Heinrich Langmann, and Harald Wagner. Moreover, the IMO 2009 had a large team of active helpers: coordinators, team guides, volunteers, and many more — not to forget the many sponsors! We would like to thank them all.

Finally, M.L. would like to thank everyone who made the last year in Bremen possible and, above all, such an enjoyable time.

D.S. would like to thank his students and colleagues for their understanding when he was sometimes preoccupied while editing this book. And of course thank you, Anke and Diego, for your support and understanding all along, and for being with me.

Structure and Randomness in the Prime Numbers

Terence Tao

Abstract. We give a quick tour through some topics in analytic prime number theory, focusing in particular on the strange mixture of order and chaos in the primes. For instance, while primes do obey some obvious patterns (e.g. they are almost all odd), and have a very regular asymptotic distribution (the prime number theorem), we still do not know a deterministic formula to quickly generate large numbers guaranteed to be prime, or to count even very simple patterns in the primes, such as twin primes $p, p+2$. Nevertheless, it is still possible in some cases to understand enough of the structure and randomness of the primes to obtain some quite nontrivial results.

1 Introduction

The prime numbers $2, 3, 5, 7, \ldots$ are one of the oldest topics studied in mathematics. We now have a lot of intuition as to how the primes *should* behave, and a great deal of confidence in our conjectures about the primes... but we still have a great deal of difficulty in *proving* many of these conjectures! Ultimately, this is because the primes are believed to behave *pseudorandomly* in many ways, and not to follow any simple pattern. We have many ways of establishing that a pattern exists... but how does one demonstrate the *absence* of a pattern?

In this article I will try to convince you why the primes are believed to behave pseudorandomly, and how one could try to make this intuition rigorous. This is only a small sample of what is going on in the subject; I am omitting many major topics, such as sieve theory or exponential sums, and am glossing over many important technical details.

Terence Tao
Department of Mathematics, UCLA, Los Angeles CA 90095-1555, USA.
e-mail: tao@math.ucla.edu

D. Schleicher, M. Lackmann (eds.), *An Invitation to Mathematics*,
DOI 10.1007/978-3-642-19533-4_1,

2 Finding Primes

It is a paradoxical fact that the primes are simultaneously very numerous, and hard to find. On the one hand, we have the following ancient theorem [2]:

Theorem 1 (Euclid's Theorem). *There are infinitely many primes.*

In particular, given any k, there exists a prime with at least k digits. But there is no known *quick* and *deterministic* way to locate such a prime! (Here, "quick" means "computable in a time which is polynomial in k".) In particular, there is no known (deterministic) formula that can quickly generate large numbers that are guaranteed to be prime. Currently, the largest known prime is $2^{43,112,609} - 1$, about 13 million digits long [3].

On the other hand, one can find primes quickly by *probabilistic* methods. Indeed, any k-digit number can be tested for primality quickly, either by probabilistic methods [10, 12] or by deterministic methods [1]. These methods are based on variants of Fermat's little theorem, which asserts that $a^n \equiv a \bmod n$ whenever n is prime. (Note that $a^n \bmod n$ can be computed quickly, by first repeatedly squaring a to compute $a^{2^j} \bmod n$ for various values of j, and then expanding n in binary and multiplying the indicated residues $a^{2^j} \bmod n$ together.)

Also, we have the following fundamental theorem [8, 14, 16]:

Theorem 2 (Prime Number Theorem). *The number of primes less than a given integer n is $(1 + o(1))\frac{n}{\log n}$, where $o(1)$ tends to zero as $n \to \infty$.*

(We use log to denote the natural logarithm.) In particular, the probability of a randomly selected k-digit number being prime is about $\frac{1}{k \log 10}$. So one can quickly find a k-digit prime with high probability by randomly selecting k-digit numbers and testing each of them for primality.

Is Randomness Really Necessary? To summarize: We do not know a quick way to find primes *deterministically*. However, we have quick ways to find primes *randomly*.

On the other hand, there are major conjectures in complexity theory, such as P = BPP, which assert (roughly speaking) that any problem that can be solved quickly by probabilistic methods can also be solved quickly by deterministic methods.[1]

These conjectures are closely related to the more famous conjecture P ≠ NP, which is a USD $ 1 million Clay Millennium prize problem.[2]

[1] Strictly speaking, the P = BPP conjecture only applies to *decision problems* — problems with a yes/no answer —, rather than *search problems* such as the task of finding a prime, but there are variants of P = BPP, such as P = promise-BPP, which would be applicable here.

[2] The precise definitions of P, NP, and BPP are quite technical; suffice to say that P stands for "polynomial time", NP stands for "non-deterministic polynomial time", and BPP stands for "bounded-error probabilistic polynomial time".

Many other important probabilistic algorithms have been *derandomised* into deterministic ones, but this has not been done for the problem of finding primes. (A massively collaborative research project is currently underway to attempt this [11].)

3 Counting Primes

We've seen that it's hard to get a hold of any single large prime. But it is easier to study the set of primes *collectively* rather than one at a time.

An analogy: it is difficult to locate and count all the grains of sand in a box, but one can get an estimate on this count by *weighing* the box, subtracting the weight of the empty box, and dividing by the average weight of a grain of sand. The point is that there is an easily measured statistic (the weight of the box with the sand) which reflects the *collective* behaviour of the sand.

For instance, from the *fundamental theorem of arithmetic* one can establish *Euler's product formula*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots\right) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} \quad (1)$$

for any $s > 1$ (and also for other complex values of s, if one defines one's terms carefully enough).

The formula (1) links the collective behaviour of the primes to the behaviour of the *Riemann zeta function*

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \ ,$$

thus

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right) = \frac{1}{\zeta(s)} \ . \quad (2)$$

One can then deduce information about the primes from information about the zeta function (and in particular, its zeroes).

For instance, from the divergence of the harmonic series $\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$ we see that $\frac{1}{\zeta(s)}$ goes to zero as s approaches 1 (from the right, at least). From this and (2) we already recover Euclid's theorem (Theorem 1), and in fact obtain the stronger result of Euler that the sum $\sum_p \frac{1}{p}$ of reciprocals of primes diverges also.[3]

In a similar spirit, one can use the techniques of complex analysis, combined with the (non-trivial) fact that $\zeta(s)$ is never zero for $s \in \mathbb{C}$ when

[3] Observe that $\log 1/\zeta(s) = \log \prod_p (1 - p^{-s}) = \sum_p \log(1 - p^{-s}) \geq -2 \sum_p p^{-s}$.

$\mathrm{Re}(s) \geq 1$, to establish the prime number theorem (Theorem 2) [16]; indeed, this is how the theorem was originally proved [8, 14] (and one can conversely use the prime number theorem to deduce the fact about the zeroes of ζ).

The famous *Riemann hypothesis* asserts that $\zeta(s)$ is never zero when[4] $\mathrm{Re}(s) > 1/2$. It implies a much stronger version of the prime number theorem, namely that the number of primes less than an integer $n > 1$ is given by the more precise formula[5] $\int_0^n \frac{dx}{\log x} + O(n^{1/2} \log n)$, where $O(n^{1/2} \log n)$ is a quantity which is bounded in magnitude by $Cn^{1/2} \log n$ for some absolute constant C (for instance, one can take $C = \frac{1}{8\pi}$ once n is at least 2657 [13]). The hypothesis has many other consequences in number theory; it is another of the USD $ 1 million Clay Millennium prize problems. More generally, much of what we know about the primes has come from an extensive study of the properties of the Riemann zeta function and its relatives, although there are also some questions about primes that remain out of reach even assuming strong conjectures such as the Riemann hypothesis.

4 Modeling Primes

A fruitful way to think about the set of primes is as a *pseudorandom set* — a set of numbers which is not actually random, but behaves like one.

For instance, the prime number theorem asserts, roughly speaking, that a randomly chosen large integer n has a probability of about $1/\log n$ of being prime. One can then *model* the set of primes by replacing them with a random set of integers, in which each integer $n > 1$ is selected with an independent probability of $1/\log n$; this is *Cramér's random model*.

This model is too crude, because it misses some obvious structure in the primes, such as the fact that most primes are odd. But one can improve the model to address this, by picking a model where odd integers n are selected with an independent probability of $2/\log n$ and even integers are selected with probability 0.

One can also take into account other obvious structure in the primes, such as the fact that most primes are not divisible by 3, not divisible by 5, etc. This leads to fancier random models which we believe to accurately predict the asymptotic behaviour of primes.

[4] A technical point: the sum $\sum_{n=1}^{\infty} \frac{1}{n^s}$ does not converge in the classical sense when $\mathrm{Re}(s) \leq 1$, so one has to interpret this sum in a fancier way, or else use a different definition of $\zeta(s)$ in this case; but I will not discuss these subtleties here.

[5] The Prime Number Theorem in the version of Theorem 2 says that, as $n \to \infty$, the number of correct decimal digits in the estimate $n/\log n$ tends to infinity, but it does not relate the number of correct digits to the total number of digits of $\pi(n)$. If the Riemann hypothesis is correct, then $\int_0^n dx/\log x$ correctly predicts almost half of the digits in $\pi(n)$.

For example, suppose we want to predict the number of twin primes n, $n+2$, where $n \leq N$ for a given threshold N. Using the Cramér random model, we expect, for any given n, that $n, n+2$ will simultaneously be prime with probability $\frac{1}{\log n \log(n+2)}$, so we expect the number of twin primes to be about[6]

$$\sum_{n=1}^{N} \frac{1}{\log n \log(n+2)} \approx \frac{N}{\log^2 N} .$$

This prediction is inaccurate; for instance, the same argument would also predict plenty of pairs of *consecutive* primes $n, n+1$, which is absurd. But if one uses the refined model where odd integers n are prime with an independent probability of $2/\log n$ and even integers are prime with probability 0, one gets the slightly different prediction

$$\sum_{\substack{1 \leq n \leq N \\ n \text{ odd}}} \frac{2}{\log n} \times \frac{2}{\log(n+2)} \approx 2 \frac{N}{\log^2 N} .$$

More generally, if one assumes that all numbers n divisible by some prime less than a small threshold w are prime with probability zero, and are prime with a probability of $\prod_{p<w}(1-\frac{1}{p})^{-1} \times \frac{1}{\log n}$ otherwise, one is eventually led to the prediction

$$2 \left(\prod_{\substack{p<w \\ p \text{ odd}}} \frac{p-2}{p} \left(1-\frac{1}{p}\right)^{-2} \right) \frac{N}{\log^2 N} = 2 \left(\prod_{\substack{p<w \\ p \text{ odd}}} \left(1 - \frac{1}{(p-1)^2}\right) \right) \frac{N}{\log^2 N}$$

(for p an odd prime, among p consecutive integers, only $p-2$ have a chance to be the smaller number in a pair of twin primes). Sending $w \to \infty$, one is led to the asymptotic prediction

$$\Pi_2 \frac{N}{\log^2 N}$$

for the number of twin primes less than N, where Π_2 is the *twin prime constant*

$$\Pi_2 := 2 \prod_{p \text{ odd prime}} \left(1 - \frac{1}{(p-1)^2}\right) \approx 1.32032\ldots .$$

For $N = 10^{10}$, this prediction is accurate to four decimal places, and is believed to be asymptotically correct. (This is part of a more general conjecture, known as the *Hardy-Littlewood prime tuples conjecture* [9].)

[6] We use the symbol $\approx$ in the sense that the quotient of the two quantities tends to 1 as $N \to \infty$.

Similar arguments based on random models give convincing heuristic support for many other conjectures in number theory, and are backed up by extensive numerical calculations.

5 Finding Patterns in Primes

Of course, the primes are a deterministic set of integers, not a random one, so the predictions given by random models are not rigorous. But can they be made so?

There has been some progress in doing this. One approach is to try to classify all the possible ways in which a set could *fail* to be pseudorandom (i.e. it does something noticeably different from what a random set would do), and then show that the primes do not behave in any of these ways.

For instance, consider the *odd Goldbach conjecture*: every odd integer larger than five is the sum of three primes. If, for instance, all large primes happened to have their last digit equal to one, then Goldbach's conjecture could well fail for some large odd integers whose last digit was different from three. Thus we see that the conjecture could fail if there was a sufficiently strange "conspiracy" among the primes.

However, one can rule out this particular conspiracy by using the *prime number theorem in arithmetic progressions*, which tells us that (among other things) there are many primes whose last digit is different from 1. (The proof of this theorem is based on the proof of the classical prime number theorem.)

Moreover, by using the techniques of *Fourier analysis* (or more precisely, the *Hardy-Littlewood circle method*), we can show that *all* the conspiracies which could conceivably sink Goldbach's conjecture (for large integers, at least) are broadly of this type: an unexpected "bias" for the primes to prefer one remainder modulo 10 (or modulo another base, which need not be an integer), over another.

Vinogradov [15] eliminated each of these potential conspiracies, and established *Vinogradov's theorem*: every sufficiently large odd integer is the sum of three primes.[7] This method has since been extended by many authors, to cover many other types of patterns; for instance, related techniques were used by Ben Green and myself [4] to establish that the primes contain arbitrarily long arithmetic progressions, and in subsequent work of Ben Green, myself, and Tamar Ziegler [5, 6, 7] to count a wide range of other additive patterns also. (Very roughly speaking, known techniques can count additive patterns that involve two independent parameters, such as arithmetic progressions $a, a+r, \ldots, a+(k-1)r$ of a fixed length k.)

[7] Vinogradov himself could not specify explicitly what "sufficiently large" is. Soon after, his student Borozdin showed that numbers greater than $3^{3^{15}} \approx 10^{6\,846\,169}$ are "sufficiently large". Meanwhile, this bound has been lowered to $e^{3\,100} \approx 10^{1\,346}$ — still far beyond reach for computer tests for the smaller numbers.

Unfortunately, "one-parameter" patterns, such as twins $n, n+2$, remain stubbornly beyond current technology. There is still much to be done in the subject!

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P. *Annals of Mathematics (2)* **160**, 781–793 (2004)

[2] Euclid, *The Elements*, circa 300 BCE

[3] Great Internet Mersenne Prime Search. http://www.mersenne.org (2008)

[4] Ben Green and Terence Tao, The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics* **167**(2), 481–547 (2008)

[5] Ben Green and Terence Tao, *Linear equations in primes*. Preprint. http://arxiv.org/abs/math/0606088, 84 pages (April 22, 2008)

[6] Ben Green and Terence Tao, *The Möbius function is asymptotically orthogonal to nilsequences*. Preprint. http://arxiv.org/abs/0807.1736, 22 pages (April 26, 2010)

[7] Ben Green, Terence Tao and Tamar Ziegler, *The inverse conjecture for the Gowers norm*. Preprint

[8] Jacques Hadamard, Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bulletin de la Société Mathématique de France* **24**, 199–220 (1896)

[9] Godfrey H. Hardy and John E. Littlewood, Some problems of 'partitio numerorum'. III. On the expression of a number as a sum of primes. *Acta Mathematica* **44**, 1–70 (1923)

[10] Gary L. Miller, Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences* **13**(3), 300–317 (1976)

[11] Polymath4 project: Deterministic way to find primes. http://michaelnielsen.org/polymath1/index.php?title=Finding_primes

[12] Michael O. Rabin, Probabilistic algorithm for testing primality. *Journal of Number Theory* **12**, 128–138 (1980)

[13] Lowell Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Mathematics of Computation* **30**, 337–360 (1976)

[14] Charles-Jean de la Vallée Poussin, Recherches analytiques de la théorie des nombres premiers. *Annales de la Société scientifique de Bruxelles* **20**, 183–256 (1896)

[15] Ivan M. Vinogradov, The method of trigonometrical sums in the theory of numbers (Russian). *Travaux de l'Institut Mathématique Stekloff* **10** (1937)

[16] Don Zagier, Newman's short proof of the prime number theorem. *American Mathematical Monthly* **104**(8), 705–708 (1997)

How to Solve a Diophantine Equation

Michael Stoll

Abstract. We introduce Diophantine equations and show evidence that it can be hard to solve them. Then we demonstrate how one can solve a specific equation related to numbers occurring several times in Pascal's Triangle with state-of-the-art methods.

1 Diophantine Equations

The topic of this text is *Diophantine Equations*. A Diophantine equation is an equation of the form

$$F(x_1, x_2, \dots, x_n) = 0\,,$$

where F is a polynomial with integer coefficients, and one asks for solutions in *integers* (or rational numbers, depending on the problem). They are named after Diophantos of Alexandria on whom not much is known with any certainty. Most likely he lived around 300 AD. He wrote the *Arithmetika*, a text consisting of 13 books, a number of which have been preserved. In this text, he explains through many examples ways of solving certain kinds of equations like the above in rational numbers. Diophantos was also one of the first to introduce symbolic notation for the powers of an indeterminate.

To give you a flavor of this kind of question, let me show you some examples. Ideally, you should cover up the part of the page below the equation and try to find a solution for yourself before you read on. The first equation

Michael Stoll
Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.
e-mail: Michael.Stoll@uni-bayreuth.de

D. Schleicher, M. Lackmann (eds.), *An Invitation to Mathematics*,
DOI 10.1007/978-3-642-19533-4_2,

is

$$x^3 + y^3 + z^3 = 29\,,$$

an equation in three unknowns, to be solved in (not necessarily positive) integers. I trust it did not take you very long to come up with a solution like $(x, y, z) = (3, 1, 1)$ or maybe $(4, -3, -2)$. Now let us look at

$$x^3 + y^3 + z^3 = 30\,.$$

Try to solve it for a while before you look up a solution in this footnote[1]. This solution is the smallest and was found by computer search in July 1999 and published in 2007 [1]. This already indicates that it may be quite hard to find a solution to a given Diophantine equation. Now consider

$$x^3 + y^3 + z^3 = 31\,.$$

Did you try to solve it? You should have come to the conclusion that there is no solution: the third power of an integer is always $\equiv -1, 0$ or $1 \bmod 9$, so a sum of three cubes can never be $\equiv 4$ or $5 \bmod 9$. Since $31 \equiv 4 \bmod 9$, the number 31 cannot be a sum of three cubes. If we replace 31 with 32, the same argument applies. So we consider

$$x^3 + y^3 + z^3 = 33$$

next. If you were able to solve this, you should consider making Diophantine equations your research area. The sad state of affairs is that it is an open problem whether this equation has a solution in integers or not![2]

So the following looks like an interesting problem: to decide if a given Diophantine equation is solvable or not. In fact, this problem appears on the most famous list of mathematical problems, namely the 23 problems David Hilbert stated in his address to the International Congress of Mathematicians in Paris in 1900 as questions worth working on in the new century. The description of the tenth problem in Hilbert's list reads thus (in the German original [3], see [4] for an English translation of Hilbert's address):

> 10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.
>
> Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

[1] $x = 2\,220\,422\,932, \quad y = -2\,218\,888\,517, \quad z = -283\,059\,965.$

[2] This introduction was inspired by a talk Bjorn Poonen gave at a workshop in Warwick in 2008.

Here is an English translation.

> Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

In modern terminology, Hilbert asks for an *algorithm* that, given an arbitrary polynomial $F(x_1, \ldots, x_n)$ with integral coefficients, decides whether the equation

$$F(x_1, \ldots, x_n) = 0$$

can be solved in integers. This is commonly known as *Hilbert's Tenth Problem*. It is not only the shortest problem on Hilbert's list, it is also the only decision problem[3], so it is somewhat special. From the wording it can be inferred that Hilbert believed in a positive solution to his problem: such an algorithm had to exist. In fact, at the end of the introductory part of his speech, before turning to the list of problems, he says

> ... in der Mathematik giebt es kein Ignorabimus!

(There is no 'Ignorabimus'[4] in mathematics.) This indicates that Hilbert was convinced that every mathematical problem must have a definite solution.

The simple examples I have shown at the beginning may (or should) have given you a feeling that this problem may actually be very hard. This is also what happened historically. People got more and more convinced that the answer to Hilbert's Tenth Problem was likely to be negative: an algorithm conforming to the given specification does not exist. Now if an algorithm does exist that performs a certain task, it is fairly clear how one can prove this fact. Namely, one has to find such an algorithm and write it down, then everybody will agree that it indeed *is* an algorithm solving the given problem. To show that such an algorithm *does not* exist is a quite different matter. One needs some way of getting a handle on all possible algorithms, so that one can show that none of them solves the problem. The relevant theory, which is a branch of mathematical logic, did not yet exist when Hilbert gave his talk. It was developed a few decades later, leading to such famous results as Gödel's Incompleteness Theorem, which definitely showed that there is an *Ignorabimus* in mathematics. Indeed, work of several people, most notably Martin Davis, Hilary Putnam and Julia Robinson, made it possible for Yuri Matiyasevich to finally prove in 1970 the following result.[5]

Theorem 1 (Davis, Putnam, Robinson; Matiyasevich).
The solvability of Diophantine equations is undecidable.

[3] A *decision problem* asks for an algorithm that decides if a given element of a specified set has a specified property.

[4] This Latin word means 'we will not know'.

[5] See [6] for an accessible account of the problem and its solution.

In fact, he proved a much stronger result, which implies for example that there is an explicit polynomial $F(x_0, x_1, \dots, x_n)$ such that there is no algorithm that, given $a \in \mathbb{Z}$ as input, decides whether or not there is an integral solution to

$$F(a, x_1, \dots, x_n) = 0\,.$$

Note that if a Diophantine equation is solvable, then we can prove it, since we will eventually find a solution by searching through the countably many possibilities (but we do not know beforehand how far we have to search). So the really hard problem is to prove that there are no solutions when this is the case. A similar problem arises when there are finitely many solutions and we want to find them all. In this situation one expects the solutions to be fairly small.[6] So usually it is not so hard to find all solutions; what is difficult is to show that there are no others.

So, given Theorem 1, should we give up all attempts to solve Diophantine equations, convinced that the task is completely hopeless? That would be premature. We might still be able to prove positive results when we restrict the set of equations in some way. For example, there are quite good reasons to believe that there should be a positive answer to Hilbert's question for equations *in two variables*. In the remainder of this contribution, we will consider one such equation as an example case and show with what kind of methods it can be attacked and solved.

2 The Example Equation

The equation we want to consider here is motivated by the following question. Consider Pascal's Triangle (Fig. 1). Which natural numbers occur several times in this triangle, if we disregard the outer two "layers" $(1, 1, 1, \dots$ and $1, 2, 3, \dots)$ on either side and the obvious reflectional symmetry?

In other words, what are the integral solutions to the equation

$$\binom{y}{k} = \binom{x}{l}\,, \tag{1}$$

subject to the conditions $1 < k \le y/2$, $1 < l \le x/2$ and $k < l$?

[6] The large solution to $x^3 + y^3 + z^3 = 30$ is no counterexample to this statement, since there should be infinitely many solutions in this case.