Peter Paule *Editor*

Mathematics, Computer Science and Logic - A Never Ending Story

The Bruno Buchberger Festschrift

RISC

Springer

Mathematics, Computer Science and Logic - A Never Ending Story

Peter Paule
Editor

Mathematics, Computer Science and Logic - A Never Ending Story

The Bruno Buchberger Festschrift

Springer

RISC

Editor
Peter Paule
Research Institute for Symbolic
Computation
Johannes Kepler University
Linz, Austria

ISBN 978-3-319-00965-0 ISBN 978-3-319-00966-7 (eBook)
DOI 10.1007/978-3-319-00966-7
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013949176

Printed on acid-free paper

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

Preface

Bruno Buchberger passed the milestone of his 60th birthday on October 22, 2002.

All the contributors to this book helped to celebrate this event, by presenting invited talks at the birthday conference "Logic, Mathematics and Computer Science - LMCS2002" presented in Professor Buchberger's renovated medieval castle at RISC in Hagenberg, Austria. Because of the superb spirit and the success of this symposium, the idea was launched to make these talks available to a larger audience. After more than a decade, the plan has finally come true, in the form of this collection of mathematical essays. Two of them are almost unchanged versions of the LMCS2002 talks: Stephen Wolfram's "New Directions in the Foundations of Mathematics" and Doron Zeilberger's "Towards a Symbolic Computational Philosophy (and Methodology!) for Mathematics". The essay "On the Role of Logic and Algebra in Software Engineering" by Manfred Broy is a slightly edited version of his LMCS2002 talk. Henk Barendregt significantly expanded his talk on "Foundations of Mathematics from the Perspective of Computer Verifcation". In their mathematical essence all these contributions are still fully up-to-date, and they rekindle the inspiring atmosphere of the Buchberger Symposium.

I want to take the opportunity to thank Ralf Hemmecke for editorial assistance and, last but not least, Martin Peters and Ruth Allewelt from Springer for their help and almost infinite patience.

Hagenberg, Austria   Peter Paule
May 2013

Contents

Foundations of Mathematics from the Perspective of Computer Verification

Henk Barendregt

To Bruno Buchberger independently of any birthday

Abstract In the philosophy of mathematics one speaks about Formalism, Logicism, Platonism and Intuitionism. Actually one should add also Calculism. These foundational views can be given a clear technological meaning in the context of Computer Mathematics, that has as aim to represent and manipulate arbitrary mathematical notions on a computer. We argue that most philosophical views over-emphasize a particular aspect of the mathematical endeavor.

1 Mathematics

The ongoing creation of mathematics, that started 5 or 6 millennia ago and is still continuing at present, may be described as follows. By looking around and abstracting from the nature of objects and the size of shapes *homo sapiens* created the subjects of arithmetic and geometry. Higher mathematics later arose as a tower of theories above these two, in order to solve questions at the basis. It turned out that these more advanced theories often are able to model part of reality and have applications. By virtue of the quantitative, and even more qualitative, expressive force of mathematics, every science needs this discipline. This is the case in order to formulate statements, but also to correct conclusions (Fig. 1).

H. Barendregt (✉)
Nijmegen University, Nijmegen, The Netherlands
e-mail: henk@cs.ru.nl

P. Paule (ed.), *Mathematics, Computer Science and Logic - A Never Ending Story*,
DOI 10.1007/978-3-319-00966-7_1, © Springer International Publishing Switzerland 2013

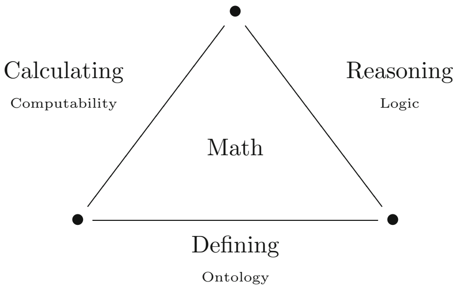

Fig. 1 The triangle of mathematical activities

The mathematical endeavor consists in a stylized way of three activities[1]: *defining*, *calculating* and *proving*.[2] The three started in this order, but over the centuries they became more and more intertwined. Indeed, before one can do arithmetic, one has to have numbers and an analogous statement holds for geometry. Having numbers one wants to add and multiply these; having polygons one wants to calculate their area. At some point the calculations became complex and one discovered shortcuts. One role of proofs is that they are an essential tool to establish the correctness of calculations and constructions.

1.1 Egyptian-Chinese-Babylonian vs Greek Mathematics

Different appreciations of the three sides of the triangle of mathematical activities gave rise to various explicit foundational views. Before entering into these we will argue that different implicit emphases on the sides of the triangle also did lead to different forms of mathematics. In the Egyptian-Chinese-Babylonian tradition emphasis was put on calculation. One could solve e.g. linear and quadratic equations. This was done in a correct way, but a developed notion of proof was lacking. In the Greek tradition the emphasis was on proofs. Using these one can show that there are infinitely many primes, or that $\sqrt{2}$ is irrational, something impossible to do by mere computation alone. But the rigor coming from geometric proofs also had its limitations. Euclid[3] [51] gives a geometric proof that $(x + y)^2 = x^2 + 2xy + y^2$, but no similar results for $(x + y)^3$ (although such a result could have been proved geometrically) or $(x + y)^4$, let alone $(x + y)^n$.

[1] I learned this from Gilles Barthe (1996, personal communication).

[2] The activity of *solving* can be seen as a particular instance of computing (or of proving, namely that of an existential statement $\exists x.P(x)$ in a constructive setting).

[3] App. 325–265 BC.

Then came Archimedes (287–212 BC), who was well versed in both calculating and proving. Another person developing mathematics toward the synthesis of these two traditions was the Persian mathematician al-Khowârizmî (app. 780–850 AD), who showed that the algorithms for addition and multiplication of decimal numbers (as we learn them at school) are provably correct.

When calculus was invented by Newton (1643–1727) and Leibniz (1646–1716) the dichotomy between proving and computing was reinforced. Newton derived Kepler's laws of planetary movement from his own law of gravitation. For this he had to develop calculus and use it in a nontrivial way. He wanted to convince others of the correctness of what he did, and went in his Principia into great detail to arrive at his conclusions geometrically, i.e. on the Greek tradition.[4] Leibniz [83] on the other hand used calculus with a focus on computations. For this he invented the infinitesimals, whose foundation was not entirely clear. But the method worked so well that this tradition still persists in physics textbooks. Euler could do marvelous things with this computational version of calculus, but he needed to use his good intuitio in order to avoid contradictions. Mathematicians in Britain, on the other hand, "did fall behind" by the Greek approach of Newton, as stated by Kline (1908–1992) [77], pp. 380–381. Only in the nineteenth century, by the work of

[4] Newton also did many important things for the synthesis of the two styles of doing mathematics. His binomial formula $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$ involves computing and reasoning. It also makes sense for n a rational number. Also his fast method of computing digits of π, see [96] or [21] pp. 142–143, is impressive. By computing twice

$$\int_0^{\frac{1}{4}} \sqrt{x-x^2}dx,$$

one time using calculus, another time using planar geometry and employing the binomial formula for $n=\frac{1}{2}$, Newton derived

$$\begin{aligned}\pi &= 24(\frac{\sqrt{3}}{32}+\frac{1}{12}-\frac{1}{160}-\frac{1}{3{,}584}-\frac{1}{36{,}864}-\frac{5}{1{,}441{,}792}-\frac{7}{13{,}631{,}488}\ldots)\\ &= 24(\frac{\sqrt{3}}{32}+\frac{1}{3}\frac{1}{2^2}-\frac{1}{5}\frac{1}{2^5}-\frac{1}{7}\frac{1}{2^9}-\frac{1}{9}\frac{1}{2^{12}}-\sum_{k=4}^{\infty}\frac{2k-3}{(2k+1)2^{3k+5}}),\end{aligned}$$

using modern notation. Newton knew how to compute $\sqrt{3}$ and this series converges quite fast. In this way he obtained $\pi = 3.14159265897928$, the last two digits are a roundoff error for 32. Ludolph van Ceulen (1539–1610) spent several decades of his life in order to compute 32 digits (later 35 digits published on his tomb in Leiden), see his [119], while with Newton's method this could have been done in a day or so. As opposed to Newton it should be admitted that van Ceulen was more precise about the validity of the digits he obtained.

Cauchy (1789–1857) and Weierstrass[5] (1815–1897), the computational and proving styles of doing calculus were unified and mathematics flourished as never before.[6]

In the last third of the twentieth century the schism between computing and proving reappeared. Computer Algebra Systems are good at symbolic computing, but they cannot keep track of assumptions and use them to check whether the side conditions necessary for certain computations actually hold, nor provide proofs of the correctness of their results. Proof-verification Systems at first were not good at computing and at providing proofs for the correctness of the result of a computation. This situation is changing now.

1.2 Progress on Foundations

During the development of mathematics, notations have been introduced to help the mathematicians to remember what they defined and how, and what they did compute and prove. A particularly useful notation came from Vieta (1540–1603), who introduced variables to denote arbitrary quantities. Together with the usual notations for the algebraic operations of addition and multiplication, this made finding solutions to numerical problems easier. The force of calculus consists for a good part in the possibility that functions can be manipulated in a symbolic way.

During the last 150 years general formal systems have been introduced for defining, computing and reasoning. These are the formal systems for ontology, computability and logic. The mathematical notations that had been used throughout the centuries now obtained a formal status. If a student who states the Archimedian axiom as "For all x and all $\epsilon>0$ there exists an $n \in \mathbb{N}$ such that $n\epsilon$ is bigger" a teacher could say only something like: "I do not exactly understand you." If the student is asked to use a formal statement to express what he or she means and answers "$\forall x \forall \epsilon>0\, \exists n \in \mathbb{N}. n\epsilon>$" the teacher can now say that this is demonstrably not a WFF (well formed formula). This little example is enough to show that these

[5] Poincaré (1854–1912) made a distinction between logicians using "Analysis", among which he placed Weierstrass, and intuitive mathematicians, using "Synthesis", like Klein. He mentioned that the intuitive mathematicians are better in discovery, although some logicians have this capacity as well. Poincaré added that we need both types of mathematicians: *Les deux sortes d'esprits sont également nécessaires aux progrès de la science; les logiciens, comme les intuitifs, ont fait de grandes choses que les autres n'auraient pas pu faire. Qui oserait dire s'il aimerait mieux que Weierstrass n'eût jamais écrit, ou s'il préférerait qu'il n'y eût pas eu de Riemann?* See [102], Chap. 1: L'intuition et la logique en mathématiques.

[6] In the nineteenth century the infinitesimals of Leibniz were abolished (at least in mainstream mathematics). But in the twentieth century they came back as *non-standard* reals. One way of doing this is by considering $h > 0$ as infinitesimal if $\forall n \in \mathbb{N}. h<\frac{1}{n}$; for this it is necessary to work in a non-Archimedian extension of $\mathbb{R}$, which can be obtained as $\mathbb{R}^I/D$, where I is an infinite set and D is an ultra-filter on $\mathcal{P}(I)$. This approach is due to Robinson (1918–1974), see his [105]. The other way consist of infinitesimals $h > 0$, such that $h^2 = 0$. This time the trick is to work in an intuitionistic context where the implication $h^2 = 0 \;\Rightarrow\; h = 0$ does not hold, see [94] and [23].