About Open Problems

Çetin Kaya Koç

Abstract A small group of computer scientists and mathematicians from industry and academia convened in a historical home ("Said Halim Pasha Palace") overlooking the Bosphorus Straits to discuss several difficult problems they and others in similar fields are tackling. The motivation of the *Open Problems in Mathematical and Computational Sciences Conference* was to enable and encourage the academic community, particularly young researchers and Ph.D. candidates, to hear about unsolved, open problems in mathematical and computation sciences, directly from the scientists who are rigorously investigating them.

1 The Conference

In general, scientists go to conferences to present discoveries that are already made, to explain results or to expose and excite the community about connections within various theories or structures, and to share their insights and proofs. Conferences are places where we get to see and hear about solutions, ask questions about them, and hope to understand them better in this process. Rarely is there an opportunity to talk about problems that have not been solved yet or solutions which are not yet satisfactory, except during the lunches, coffee breaks, or at other quiet times.

In many instances, scientists working on problems whose solutions are difficult to obtain will state that asking the right question is the real challenge. It is imperative to stop and think once in a while in order to understand the background of the tools and the mechanisms needed for tackling the problems we are working on. Conferences that deal with open problems are rare, but they are useful avenues for such objectives. Almost all conferences are for presenting the solutions to certain classes of problems whose origins we may not have any idea about.

Ç.K. Koç (✉)
University of California Santa Barbara, Santa Barbara, CA 93106, USA

Mathematical and Computational Sciences Labs, TÜBİTAK BİLGEM, Gebze, Kocaeli, Turkey
e-mail: koc@cs.ucsb.edu

Ç.K. Koç (ed.), *Open Problems in Mathematics and Computational Science*,
DOI 10.1007/978-3-319-10683-0_1

In a world replete with information, what matters most is sometimes not the answers but rather the context, the origin and the body of questions for which answers are sought or obtained.

This conference was planned with these ideas in mind. One purpose of the *Open Problems in Mathematical and Computational Sciences Conference* is to encourage, motivate, and excite the mathematical and computational sciences community to discuss open problems. We would like to hear them formulate the questions and present processes which will be helpful in the quest for answers.

Of course, we all know about certain open problems or conjectures in mathematics such as the Goldbach conjecture or the twin primes conjecture or the Riemann hypothesis. Some well-known problems have been resolved during the last 20 years, three excellent examples being Fermat's last theorem by Andrew Weil in 1995, the Poincaré conjecture by Grigori Perelman in 2003, and the prime gap problem by Yitang Zhang (and later by the Polymath Project participants) in 2013. The list of difficult problems in mathematics is pretty long, and solutions come in decades or even centuries. And when they come, they are deservedly celebrated, and the international media and thus the public pay attention; stories are made and impressions are created. Furthermore, mathematics institutes around the world, for example, the Clay Institute, publish problem lists and offer prizes which further publicize the phenomena.

However, we are limiting our attention to computational problems in this conference; there is also a long list of unsolved problems in computer science, such as:

- P = NP problem
- Existence of one-way functions
- Is the graph isomorphism problem in P?
- Is factoring in P?
- Is primality testing in P?
- What is the fastest algorithm for the multiplication of integers?
- What is the fastest algorithm for matrix multiplication?

The list is not complete, and our intention is not to complete the list, but to bring the best minds to describe, elucidate, and explain some of these open problems in the mathematical and computational sciences, particularly the problems they themselves are interested in or working on or for which they have formulated partial or near-complete solutions. We want them to tell us how they approach such problems and what are the mechanisms and tools they are using and share with us and excite us with the creative energy they are applying to such problems.

A perfect example from the above list was the question "Is Primality Testing in P?" This was affirmatively answered by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena of the Indian Institute of Technology Kanpur, by giving the first deterministic polynomial time algorithm for primality testing. The implications of this development are indeed great for cryptography, coding, and finite fields, where primality plays a central role.

To summarize, one of the underlying purposes of our 3-day conference was to encourage young researchers, particularly Ph.D. candidates, to learn about exciting, interesting, and important (yet) unsolved problems in mathematical and computation sciences, directly from the researchers who are thinking about them. I believe the informal atmosphere of the conference allowed them to listen to the seminars, ask questions, interact, and discuss possible answers or pose new questions to the invited speakers.

We believe such a close interactive environment served as a catalyzing event and hopefully will synchronize local research communities with the best, most challenging, and perhaps most useful problems the world's best minds are working on. Hopefully, in several years, perhaps even as early as the next Open Problems Conference, a few of these challenging problems will find their partial or complete solutions.

2 The Participants

The following people attended the conference as invited speakers:

- Paulo Barreto, Universidade de Sao Paulo
- Claude Carlet, Université Paris 8
- Guanrong Chen, City University of Hong Kong
- Ömer Eğecioğlu, University of California, Santa Barbara
- Gerhard Frey, Göttingen Academy of Sciences
- Tor Helleseth, University of Bergen
- Antoine Joux, Université de Versailles Saint-Quentin-en-Yvelines
- Andrew Klapper, University of Kentucky
- Alfred Menezes, University of Waterloo
- David Naccache, Université Paris II
- Koji Nakano, Hiroshima University
- Ferruh Özbudak, Middle East Technical University
- Daniel Panario, Carleton University
- Bart Preneel, KU Leuven
- Gheorghe Pãun, Romanian Academy
- Jean-Jacques Quisquater, Université catholique de Louvain
- Henning Stichtenoth, Sabancı University
- Murat Tekalp, Koç University
- Han Vinck, University of Duisburg-Essen

We thank our speakers for taking time to come to Istanbul to talk about problems that excite them and to share them with us. There were more than 150 participants, most of whom were from Turkey, as expected; however, about 10 % of the participants were from other European countries, including Bulgaria, Denmark, France, and Romania.

3 The Book

As we were planning the conference, we also developed a plan to publish a book arising from the presentations.

This book contains *selected and revised* papers from the conference. We gave a window of about 6 months to the speakers to create the chapters in this book, revising and expanding their work by adding an introduction section and an annotated bibliography. The introduction section of each chapter is intended to provide the background of the topic of the chapter, assuming the reader is a first-year graduate student who has the general knowledge of electrical engineering, computer science, programming, and computational mathematics via his/her undergraduate education and has just started reading books and papers in the area of the chapter. Therefore, the chapters attempt to give all basic definitions, introduce the context, and summarize algorithms, theorems, and proofs. On the other hand, the bibliography aims to introduce the most important references to follow up, giving a short description of these papers and books, and their importance to the field. I hope you will find these chapters to your liking.