For Favour of Posting

Department of Mathematics
The Institute of Mathematical Sciences
The Chinese University of Hong Kong

數學系
數學科學研究所
香港中文大學

Phone: (852) 3943 7988 • Fax: (852) 2603 5154 • Email: dept@math.cuhk.edu.hk (Math. Dept.)
Room 220, Lady Shaw Building, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong

Joint Seminar

Determining Whether Given Large Numbers Are Primes I, II

Professor Jing Yu
National Taiwan University

Part I
Date: 30 November 2018 (Friday)
Time: 2:00pm – 3:00pm
Venue: LT 3, Lady Shaw Building,
The Chinese University of Hong Kong, Shatin

Part II
Date: 3 December 2018 (Monday)
Time: 2:00pm – 3:00pm
Venue: LT 3, Lady Shaw Building,
The Chinese University of Hong Kong, Shatin

All are Welcome

Introduction to the Speaker

Prof. Jing YU got his PhD from Yale university under the guidance of Serge Lang. He has made many outstanding contributions to number theory, in particular to transcendence theory for function fields. In recognition of his achievements, he was appointed a National Chair in Natural Science of the Minister of Education, elected to an Academician of Academia Sinica, and a Fellow of the World Academy of Sciences. He is currently a professor of National Taiwan University, and a visiting Professor at CUHK under the Lee Hysan Foundation visiting programme during fall semester of 2018.

Abstract

In 1801, C. Gauss wrote: “The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.

This is even more true today, Your use of ATM card or purchase something with credit card over the Web depends on the intractability of these problems.

In a successful Undergraduate Research Project (2002), Agrawal, Kayal and Saxena from India, discovered an amazing algorithm which can recognize primes deterministically in polynomial time of the inputs. This was a great breakthrough over the two centuries. AKS thereby won Clay Research Award 2002, the ICTP Prize 2003, the 2006 Gödel Prize and the 2006 Fulkerson Prize for this work.

In these two talks, we will explain the proof of this beautiful AKS algorithm. This proof can be understood well by undergraduates. We will also relate the concepts such as: complexity estimates, P versus NP, and the distinction between certifying primes and factorization of integers.