Graduate Lecture

Primes and the Beauty of Algorithms: An Introduction

This lecture will be an introduction for graduate students to the topic of the first Colloquium talk, where we will give a survey of primality proving algorithms for various purposes, ranging from cryptographic use, general purpose primality proving algorithms and the fascinating result of Agarwal, Kayal and Saxena, to special algorithms and prime hunters' daily life.

Colloquium I

Primes and the Beauty of Algorithms

The lecture intends to provide a survey of primality proving algorithms for various purposes, ranging from cryptographic use, general purpose primality proving algorithms and the fascinating result of Agarwal, Kayal and Saxena, to special algorithms and prime hunters' daily life.

We will put in evidence the evolution and variation of the main ideas and the way they adapt to the specific primality testing aim. Finally, the diversity of algorithms and some specific phenomena which will be pointed out in due time, will lead to an interesting qualitative discussion of the limits of complexity theory as unique means for evaluating algorithms. Beauty – with its possibility to adapt to situations – emerges as a non-conceptual yet robust evaluation criterion.

Colloquium II

Cyclotomic Norm Equations

We discuss the equation

$$(X^p + Y^p)/(X + Y) = p^e Z^q \,,$$

where X, Y, Z are coprime integers and p, q are odd primes while $e = 1$ if p divides $X + Y$ and $e = 0$ otherwise. The equation specializes to various important cases, which were conjected to have no or few sporadic solutions. The method with which we treat this equations systematizes various approaches, some of which were successfully used in the proof of Catalan's equation. Altogether, the aim of the lecture is to show the force and limits of cyclotomic methods for the understanding of this equation and its special cases.