I M B M istanbul matematiksel bilimler merkezi
istanbul center for mathematical sciences

Integer multiplication and its applications

David Harvey

The University of New South Wales, Sydney, Australia

Abstract

Integer multiplication is an ancient problem, with countless applications across all fields of human endeavour. Until the late 1950s, the fastest known multiplication algorithm, asymptotically speaking, was the long multiplication method that we learn at primary school. This method requires $O(n^2)$ basic operations to calculate the product of two n-digit numbers. The current fastest algorithm, discovered by Joris van der Hoeven and myself a few years ago, calculates the same product in only $O(n \log n)$ operations.

In this talk, I will briefly discuss the history of fast multiplication algorithms, and then turn to some applications, drawn from fields such as number theory and cryptography. In particular, I will discuss a few examples of problems whose resolution depends crucially on the ability to quickly multiply enormous integers, with millions or even billions of digits.

Date : Monday, April 22, 2024
Time: 15:00
Place: Bogazici University South Campus, TB 310

Supported by