Recent developments in primality testing

Carl Pomerance
Bell Labs
Lucent Technologies

Thursday, February 6, 2003
Carson L02*, 4:00 pm
(Tea 3:30 pm Math Lounge)

Abstract

Last August, Agrawal, Kayal, and Saxena, all from the Indian Institute of Technology in Kanpur, announced a new algorithm to distinguish between prime numbers and composite numbers. Unlike earlier methods, their method is completely rigorous, deterministic, and runs in polynomial time. Previous results, some of them quite deep, were close to this ideal in various ways, so, perhaps, it was not such a great surprise that such a result should exist. But the relatively easy algorithm and proof is stunning. In this talk, the new algorithm will be described as well as some more recent developments.

This talk should be accessible to graduate students.

1044308116

*Lower level of Carson Hall, which is adjacent to Berry Library. Entry is across the street from Rockefeller.