



CHAUVENET PRIZE

The Chauvenet Prize is awarded to the author of an outstanding expository article on a mathematical topic by a member of the Association. First awarded in 1925, the prize is named for William Chauvenet, a professor of mathematics at the United States Naval Academy. It was established through a gift in 1925 from J. L. Coolidge, then MAA president. Winners of the Chauvenet Prize are among the most distinguished of mathematical expositors.

Citation

Andrew Granville

“It is easy to determine whether a given integer is prime,” *Bulletin of the American Mathematical Society (N.S.)* 42 (2005), 3–38.

This article is fascinating, readable, and understandable, with lots of proofs. The entire abstract is a totally relevant quote from Gauss! The paper includes the statement, AND PROOF, of the amazing result by Agrawal, an Indian computer scientist, and his two undergraduates, Kayal and Saxena, giving a “polynomial time deterministic” test for determining if integers are primes. The AKS algorithm (for their last names) was announced in August 2002. Efficient algorithms were already in use, and it is suspected that some of them work in polynomial time. The AKS algorithm is the first algorithm proved to work in polynomial time, and this result “has the great advantage that it is straightforward to develop into a fast algorithm for proving the primality of large primes.”

The paper includes interesting tidbits like the passage from Oliver Sacks's *The Man Who Mistook His Wife for a Hat* about a pair of severely autistic twins who could determine whether 20-digit numbers are prime, and we'll never know how because they were eventually separated and “socialized.” But we mislead: The paper is full of significant information, including discussions of Carmichael numbers, random polynomial time algorithms, probabilistic (almost) proofs, and much more. In one section, the author quickly and clearly explains the important connection between factoring integers and cryptography, and mentions the famous RSA cryptosystem. Section 7, titled “Stop the Press,” includes the fact that Lenstra and Pomerance have modified the AKS algorithm so that it works in $(\log n)^6$ polynomial time.

Biographical Note

Andrew Granville is the Canadian Research Chair in number theory at the Université de Montréal. His research focus is on any area to do with understanding the distribution of primes. Encouraged by the writings of two of his mentors, Paulo Ribenboim and Carl Pomerance, he has long been interested in

communicating these ideas to a broad audience, and this has previously been recognized by the MAA's 1995 Hasse Prize, as well as its 2007 Lester R. Ford Award.

Dr. Granville was a plenary speaker at the Annual Joint Meetings of 1996 and 2002, and this article evolved from his presentation at the Current Events special session of the 2004 Joint Mathematics Meetings. Dr. Granville helped create the questions for the MAA's Putnam exam from 1999 to 2002, has served on the scientific advisory panels of MSRI and of the Fields Institute, and has served on prize selection committees, such as for the 2005 Cole Prize and the 2008 Doob Prize.

Response from Andrew Granville

When David Eisenbud asked me to present the exciting new polynomial time primality testing algorithm of Agrawal, Kayal, and Saxena at the 2004 AMS Current Events special session in a way that would be accessible to undergraduates at the meeting yet interesting to seasoned researchers, I could not have guessed the journey this would take me on. My goal was to integrate ideas from modern computational number theory/cryptography into an analytic number theory discussion while at the same time keeping everything accessible to a keen but inexperienced reader. What started slowly began to "flow" thanks to help I received, both technical and expository—running drafts past students at various universities allowed me to identify passages that needed reworking. A book by Ribenboim and an article by Bombieri provided many ideas as to how to present several of the technically difficult ideas in an accessible way, and a website of Bernstein provided lots of background information. Pomerance, Agrawal, and others helped me find new, more accessible proofs to some of the more challenging aspects of the material. A big thanks for all of this help!