Independence of the Miller-Rabin and Lucas Probable Prime Tests

Leng, Alec

In the modern age, public-key cryptography has become a vital component for secure online communication. To implement these cryptosystems, rapid primality testing is necessary in order to generate keys. In particular, probabilistic tests are used for their speed, despite the potential for pseudoprimes. So, we examine the commonly used Miller-Rabin and Lucas tests, showing that numbers with many nonwitnesses are usually Carmichael or Lucas-Carmichael numbers in a specific form. We then use these categorizations, through a generalization of Korselt's criterion, to prove that there are no numbers with many nonwitnesses for both tests, affirming the two tests' relative independence. As Carmichael and Lucas-Carmichael numbers are in general more difficult for the two tests to deal with, we next search for numbers which are both Carmichael and Lucas-Carmichael numbers, experimentally finding none less than 10^{16}. We thus conjecture that there are no such composites and, using multivariate calculus with symmetric polynomials, begin developing techniques to prove this.

Awards Won:
American Mathematical Society: Certificate of Honorable Mention