

Samuel S. Wagstaff, Jr. (b. 21 February 1945)

[55, 408, 1967, 2021, 1, 3, 8]

Wikipedia: https://en.wikipedia.org/wiki/Samuel_S._Wagstaff_Jr.

Homepage: <https://homes.cerias.purdue.edu/~ssw>

Essay by Daniel Rogers

Samuel S. Wagstaff, Jr. is currently a professor of computer science and mathematics at Purdue University and has taught at several other institutions: the University of Rochester, the Institute for Advanced Study in Princeton, the University of Illinois in Urbana-Champaign, and the University of Georgia. In 2019, Wagstaff retired from teaching but has since remained active via writing, researching, and advising his students. He earned his Bachelor of Science at Massachusetts Institute of Technology in 1966 and his PhD at Cornell University in 1970. Wagstaff wrote his dissertation *On Infinite Matroids* with the help of his advisor Oscar S. Rothaus; his Mathematics Subject Classification was 05–Combinatorics. Wagstaff’s research interests include cryptography, parallel computation, and analysis of algorithms. His most cited publications are “The pseudoprimes to $25 * 10^9$ ” and “Factorizations of $b^n \pm 1$.” The latter of these is continued in the Cunningham Project, led by Wagstaff. His leadership in the Cunningham Project has resulted in many great strides. It also led Wagstaff to the 2003 International Conference on Number Theory for Secure Communications at SASTRA University. At this conference, he witnessed the president’s designation of Ramanujan’s house as a national treasure.

I recently had the opportunity of conducting an interview with Dr. Wagstaff via Zoom. Wagstaff considers his greatest success to be the Baillie–PSW primality test: a probabilistic

primality testing algorithm that discerns whether a number is composite or is a probable prime. Wagstaff constructed this test by combining the pseudoprime tests of Fermat and Lucas. At first, \$30 was offered for the discovery of a counterexample, and since then the prize has grown from \$30 to \$600, and \$600 to \$2,000! Wagstaff's colleague Carl Pomerance has argued that there are infinitely many counterexamples, but there are still no known Baillie–PSW pseudoprimes. According to Wagstaff, the greatest difficulty in his career is finding a polynomial time algorithm to factor integers. This unsolved problem has puzzled many mathematicians and computer scientists; there were many great advancements in Wagstaff's lifetime, but progress has recently come to a standstill. Some of Wagstaff's greatest influences are John Selfridge, D. H. Lehmer, Klaus Roth, and Carl Pomerance. Pictured below are photographs of Dr. Wagstaff at the Ramanujan Centre in Kumbakonam, India (left) and with the factorization of $3^{349} - 1/2$ (right.)

