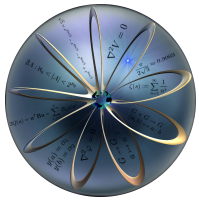

planetmath.org

Math for the people, by the people.

Carl Pomerance

Canonical name	CarlPomerance
Date of creation	2013-03-22 16:56:00
Last modified on	2013-03-22 16:56:00
Owner	PrimeFan (13766)
Last modified by	PrimeFan (13766)
Numerical id	4
Author	PrimeFan (13766)
Entry type	Biography
Classification	msc 01A60
Classification	msc 01A61
Classification	msc 01A65

Carl Pomerance (1944 -) American mathematician, discoverer of the quadratic sieve method for integer factorization, co-author with Richard Crandall of the seminal book *Prime Numbers: A Computational Perspective*.

Born in Missouri, Pomerance studied at Brown and later Harvard. After graduation in 1972, he taught at the University of Georgia for the rest of the century. He worked for four years at Lucent Technologies (now Alcatel-Lucent), then joined the math faculty of Dartmouth College at about the same time he was appointed a Fellow of the American Association for the Advancement of Science. Early in his teaching career, Pomerance was recognized with the Chauvenet Prize.

In 1978, Pomerance co-authored with Erdős a paper on the largest prime factors of n and $n+1$ in *Aequationes Math.* **17**, giving him `http://planetmath.org/ErdHosNumberl` number 1. (In 1969, when fellow Erdős number 1 collaborator Hank Aaron broke Babe Ruth's homerun record with 715, Pomerance began studying Ruth-Aaron pairs). The greatest recognition for Pomerance, however, might be that the use of his quadratic sieve method cracked RSA-129.