Finding Four Million Large Random Primes

Ronald L. Rivest*
Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139

A number n is a (base two) *pseudoprime* if it is composite and satisfies the identity

$$2^{n-1} \equiv 1 \pmod{n} . \tag{1}$$

Every prime satisifies (1), but very few composite numbers are pseudoprimes. If pseudoprimes are *very* rare, then one could even find large "industrial strength" primes (say for cryptographic use) by simply choosing large random values for n until an n is found that satisfies (1). How rare are pseudoprimes? We performed an experiment that attempts to provide an answer. We also provide some references to the literature for theoretical analyses.

Using a network of 33 SUN Sparcstations, approximately 718 million random 256-bit values were tested by a "small divisor test", followed (if the small divisor test was passed) by a test of equation (1), followed (if the equation (1) was satisified) by 8 iterations of the Miller-Rabin probabilistic primality test. A number passes the small divisor test if it has no divisors smaller than 10^4. Of the numbers tested, 43,741,404 of them passed the small-divisor test. Of those, 4,058,000 satisfied equation (1). Of those, *all* passed 8 iterations of the Miller-Rabin probabilistic primality test. That is, *no pseudoprimes were found.* In other words, every number that passed the small-divisor test and satisfied equation (1) was found to be (probably) prime. Empirically, therefore, pseudoprimes are very rare, at least among numbers with no small divisors.

The available theory also suggests that pseudoprimes are rare. On the basis of extensive experience and analysis, Pomerance [5, 8] conjectures that the number of pseudoprimes less than n is at most

$$n/L(n)^{1+o(1)} \tag{2}$$

where

$$L(n) = \exp\left(\frac{\log n \log\log\log n}{\log\log n}\right) .$$

*Supported by NSF grant CCR-8914428, and RSA Data Security. email address: rivest@theory.lcs.mit.edu

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 625-626, 1991.