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

If this conjecture is correct, and we make the (unjustified) additional assumption that the $o(1)$ in conjecture (2) can be ignored, then the number of pseudoprimes less than 2^{256} is conjectured to be at most

$$4 \times 10^{52}$$

whereas the number of 256-bit primes is approximately

$$6.5 \times 10^{74} \ .$$

Thus, if Pomerance's conjecture is correct (and if the $o(1)$ term can safely be ignored), the chance that a randomly chosen 256-bit number that satisfies equation (1) is in fact composite is less than 1 in 10^{22}. For "practical purposes" pseudoprimality may be a sufficient guarantee of primality. (Of course, it is easy to improve the test to provide higher reliability.) Our experiments are consistent with these theoretical conjectures. For further information on finding large primes and on the density of pseudoprimes, see [1, 2, 3, 4, 5, 6, 7, 8].

Acknowledgments

I'd like to thank Carl Pomerance for bringing some of his work to my attention, and William Ang for helping with the running of the programs.

References

[1] Pierre Beauchemin, Gilles Brassard, Claude Crépeau, Claude Goutier, and Carl Pomerance. The generation of random numbers that are probably prime. *Journal of Cryptology*, 1:53–64, 1988.

[2] Pomerance C., J. L. Selfridge, and S. Wagstaff, Jr. The pseudoprimes to $25 \cdot 10^9$. *Mathematics of Computation*, 35(151):1003–1026, July 1980.

[3] Paul Erdös and Carl Pomerance. On the number of false witnesses for a composite number. *Mathematics of Computation*, 46(173):259–279, January 1986.

[4] Su Hee Kim and Carl Pomerance. The probability that a random probable prime is composite. *Mathematics of Computation*, 53(188):721–741, October 1989.

[5] Carl Pomerance. On the distribution of pseudoprimes. *Mathematics of Computation*, 37(156):587–593, 1981.

[6] Carl Pomerance. A new lower bound for the pseudoprime counting function. *Illinois Journal of Mathematics*, 26(1):4–9, Spring 1982.

[7] Carl Pomerance. On the number of false witnesses for a composite number. *Mathematics of Computation*, 46(173):259–279, January 1986.

[8] Carl Pomerance. Two methods in elementary analytic number theory. In R. A. Mollin, editor, *Number Theory and Applications*, pages 135–161. Kluwer Academic Publishers, 1989.