SIAM J. COMPUT.
Vol. 6, No. 1, March 1977

A FAST MONTE-CARLO TEST FOR PRIMALITY*

R. SOLOVAY† AND V. STRASSEN‡

Abstract. Let n be an odd integer. Take a random number a from a uniform distribution on the set $\{1, 2, \cdots, n-1\}$. If a and n are relatively prime, compute the residue $\varepsilon \equiv a^{(n-1)/2} (\mathrm{mod}\ n)$, where $-1 \leqq \varepsilon < n-2$, and the Jacobi symbol $\delta = (a/n)$. If $\varepsilon = \delta$, decide that n is prime. If either gcd $(a, n) > 1$ or $\varepsilon \neq \delta$ decide that n is composite. Obviously, if n is prime, the decision made will be correct. We will show below, that for composite n the probability of an incorrect decision is $\leqq 1/2$. The number of multiprecision operations needed for the whole procedure is $< 6 \log_2 n$. m-fold repetition using independent random numbers yields a Monte-Carlo test for primality with error probabilities 0 (if n is prime) and $< 2^{-m}$ (if n is composite) and with multiprecision arithmetic cost $< 6m \log_2 n$.

Key words. Monte-Carlo tests, primality

1. Cost of the procedure. By a multiprecision operation we mean an arithmetic operation or a division with remainder of two numbers $< n^2$. To decide whether a and n are relatively prime, we compute (a, n) by Euclid's algorithm. This can be done with approximately $1.5 \log_2 n$ multiprecision operations (see Knuth [1, p. 320]). Computing ε can be done by $1.25 \log_2 n$ multiplications each followed by a reduction mod n, i.e., by $2.5 \log_2 n$ multiprecision operations (Knuth [1, p. 409]). We compute δ with the help of the reciprocity law for Jacobi symbols ([2, p. 79]). This is about as hard as computing (a, n). The total number of multiprecision operations of the procedure can therefore be estimated from above by $6 \log_2 n$.

2. Error probability. If n is prime, the procedure obviously reaches a correct decision. Let n be composite. The set

$$G = \left\{ a + (n) | a \in \mathbb{Z} \ \&\ (a, n) = 1 \ \&\ a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\ n) \right\}$$

is a subgroup of the group of units $\mathbb{Z}_n^\times$ of $\mathbb{Z}_n$. Therefore it suffices to show $G \neq \mathbb{Z}_n^\times$ (for this implies $|G| \leqq \frac{1}{2}|\mathbb{Z}_n^\times| \leqq (n-1)/2$, so that at most $\frac{1}{2}$ of the numbers between 1 and $n-1$ will lead to the decision that n is prime).

By the way of contradiction assume

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\ n) \tag{1}$$

for all $a \in \mathbb{Z}$ relatively prime to n. If $n = p^e$ is a prime power, we get from (1)

$$a^{pe-1} \equiv 1\ (\mathrm{mod}\ p^e)$$

for all a not divisible by p. Since $\mathbb{Z}_{p^e}^\times$ is cyclic of order $p^{e-1}(p-1)$ we have

$$p^{e-1}(p-1) | p^e - 1$$

* Received by the editors June 12, 1974, and in final revised form October 6, 1975.
† IBM Watson Laboratory, Yorktown Heights, New York 10598.
‡ Seminar fur Angewandte Mathematik, Universität Zurich, 8032 Zurich, Switzerland.

and therefore $e \leqq 1$, which is impossible since n is composite. Thus n has a nontrivial factorization $n = r \cdot s$ with $(r, s) = 1$. Equation (1) implies

$$a^{(n-1)/2} \equiv \pm 1 \pmod n \tag{2}$$

for all a relatively prime to n. We claim that in fact

$$a^{(n-1)/2} \equiv 1 \pmod n \tag{3}$$

for such a. Otherwise there is an a with $a^{(n-1)/2} \equiv -1 \pmod n$. Since r and s are relatively prime we can apply the Chinese remainder theorem and find b with $b \equiv 1 \pmod r$, $b \equiv a \pmod s$. Then

$$b^{(n-1)/2} \equiv 1 \pmod r, \qquad b^{(n-1)/2} \equiv -1 \pmod s,$$

in contradiction to (2). Equation (3) implies

$$\left(\frac{a}{n}\right) = 1$$

for all a relatively prime to n, which is impossible.

Remarks 1. Our result should not be confused with assertions as to n being prime or not which are correct with high probability given that n is a random number sampled from the uniform distribution on a sufficiently large segment of the integers. Under such a hypothesis it is reasonable to decide that n is composite without even looking at it. The probability of error may be further substantially reduced by checking, e.g., whether

$$2^n \equiv 2 \pmod n$$

(see Erdös [3]).

2. Perhaps it is useful to measure the complexity of a Monte-Carlo test (with one probability of error $= 0$ as above) by a single quantity. If the test has error probability α and cost t, we suggest $t/(-\log \alpha)$ as such a measure, since this is invariant under independent repetition.

Acknowledgment. It is a pleasure to thank Ernst Specker for interesting discussions about the subject.

REFERENCES

[1] D. E. KNUTH, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969.

[2] I. NIVEN AND H. S. ZUCKERMAN, *An Introduction to the Theory of Numbers*, John Wiley, New York, 1966.

[3] P. ERDÖS, *On almost primes*, Amer. Math. Monthly, 57 (1950), pp. 404–407.