SIAM J. COMPUT.
Vol. 11, No. 2, May 1982

0097-5397/82/1102-0014 $01.00/0

ON PRIMALITY TESTS*

DANIEL J. LEHMANN†

Abstract. Whether an odd number m is prime can be decided on the knowledge of the image of the function $a \mapsto a^{(m-1)/2}(m)$. As a consequence, an algorithm for testing primality is proposed (under the extended Riemann hypothesis) which is more efficient than ones proposed by Miller [Proc. 7th ACM Symp. Theory of Computing, 1975, pp. 234–239] and Vélu [SIGACT News, 10 (1978), pp. 58–59]. A probabilistic version is compared with the algorithm of Solovay and Strassen [SIAM J. Comput., 6 (1977), pp. 84–85; erratum, 7 (1978), p. 118].

Key words. primality, extended Riemann hypothesis, probabilistic algorithms

Let $(Z/mZ)^*$ be the multiplicative group of units of Z/mZ. Let $f_{n,m}:(Z/mZ)^* \to (Z/mZ)^*$ be the group homomorphism defined by $f_{n,m}(a) = a^n$. If $m = p^\alpha$ for a prime p and a positive integer α, we shall say that m is a prime power (n.b: a prime is a prime power).

LEMMA 1. *If m is not a prime power, then the image of $f_{n,m}$ is not the subgroup $\{+1, -1\}$ (it may be in that subgroup, though).*

Proof. If m is not a prime power, it is the product of two relatively prime integers greater than 1. Let $m = m_1 m_2$, $(m_1, m_2) = 1$, $m_1, m_2 > 1$. Suppose

$$f_{n,m}(a) = -1 \quad \text{for some } a \in (Z/mZ)^*.$$

Then $a^n \equiv -1 (m_1)$. By the Chinese remainder theorem, there is a (unique) $x \in (Z/mZ)^*$ such that $x \equiv a \ (m_1)$ and $x \equiv 1 \ (m_2)$. Then $f_{n,m}(x)$ is not in $\{1, -1\}$. □

THEOREM 1. *Let m be an odd integer. The image of $f_{(m-1)/2,m}$ is the subgroup $\{+1, -1\}$ if and only if m is prime.*

Proof. The *if* part follows from well-known theorems of elementary number theory. The *only if* part follows from Lemma 1 and the fact that if $m = p^\alpha$ for p a prime and $\alpha > 1$, $(Z/mZ)^*$ is cyclic of order $p^{\alpha-1}(p-1)$, which is divisible by p; if the image of $f_{m-1,m}$ were the trivial subgroup, p would divide $m - 1 = p^\alpha - 1$. □

Note that $f_{(m-1)/2,m}$ can be trivial only if m is not a prime power.

THEOREM 2 (Ankeny–Montgomery). *If the extended Riemann hypothesis is true, there is a number M such that for every integer m every Abelian group G and every nontrivial homomorphism $f:(Z/mZ)^* \to G$ there is an element a less than $M(\log m)^2$ such that $f(a) \neq 1$.*

ALGORITHM 1. For each element a of $(Z/mZ)^*$ less than $M(\log m)^2$, compute $f_{(m-1)/2,m}(a)$.

If at least one of the values found is different from 1 and -1, then m is composite. Otherwise, if at least one of the values found is -1, then m is prime and else m is composite.

Proof of correctness. If at least one of the values found is different from 1 and -1, then by Theorem 1, m is composite. If all the values found are $+1$ or -1, Theorem 2 implies that the homomorphism $g:(Z/mZ)^* \to (Z/mZ)^*/\{+1, -1\}$ defined by $g = j \circ f_{(m-1)/2,m}$, where j is the canonical projection $(Z/mZ)^* \to (Z/mZ)^*/\{+1, -1\}$, is trivial. The image of $f_{(m-1)/2,m}$ is therefore a subgroup of $\{+1, -1\}$. If the value -1 is

* Received by the editors January 24, 1979, and in revised form April 13, 1980.

† Department of Computer Science, Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel. Part of this work was done while the author was at the University of Southern California, Los Angeles, California.

found at least once, then the image is $\{+1, -1\}$ and by Theorem 1, m is prime. If all the values found are $+1$, then by Theorem 2, $f_{(m-1)/2,m}$ is trivial and by Theorem 1 m is composite. □

Algorithm 1 is more efficient than the one proposed by Vélu because it avoids computing the Jacobi function $\left(\frac{a}{m}\right)$. It is closely related to Miller's as will be shown now but seems simpler, and the number of operations involved is slightly smaller in the worst case.

To link Algorithm 1 with Miller's, let us examine in more detail the case where $f_{(m-1)/2,m}$ is trivial. In such a case, m is not a prime power. By Lemma 1, then, for any n the image of $f_{n,m}$ is either the trivial subgroup or is not included in $\{1, -1\}$. Let $m-1=2^l \cdot m'$ with m' odd. Because m' is odd, $f_{m',m}$ cannot be trivial ($f_{m',m}(-1)=-1$); there is therefore a largest $k \leqq l$ such that $f_{2^k \cdot m',m}$ is not trivial. There is an a for which $b=f_{2^k \cdot m',m}(a) \neq \pm 1$ and $b^2=f_{2^{k+1} \cdot m',m}(a)=1$. Such an a is a witness of the fact that m is not prime and even enables the factorization of m, since

$$b^2=1\ (m) \Rightarrow (b+1)(b-1)=0\ (m) \Rightarrow (b+1, m) \neq 1 \text{ or } (b-1, m) \neq 1.$$

A probabilistic version of Algorithm 1 can be given, based on the following.

LEMMA 2. *Let G_1 and G_2 be finite groups, $f: G_1 \to G_2$ a group homomorphism and G_3 a subgroup of G_2. If the image of f is not contained in G_3, then $f(a) \notin G_3$ for at least half the elements a of G_1.*

Proof. $G_3 \cap \mathrm{Im}(f)$ is a strict subgroup of $\mathrm{Im}(f)$; therefore, at least half the elements of $\mathrm{Im}(f)$ are in $\mathrm{Im}(f)-G_3$. But if the kernel of f has size k, then every element of $\mathrm{Im}(f)$ is the image of exactly k different elements of G_1. □

ALGORITHM 2. Let m be an odd integer. Draw k random elements of $(Z/mZ)^*$: $a_1, a_2, \cdots, a_k$ for each one compute $a^{(m-1)/2}$.

If at least one of the values found is different from $+1$ and -1, then m is certainly composite. If only values of $+1$ and -1 are found and the value -1 is found at least once, then m is prime with probability greater than $1-2^{-k}$. If all the values found are $+1$, then m is composite with probability greater than $1-2^{-k}$.

Proof. Immediate from Lemma 2. □

Algorithm 2 is more efficient than the one proposed by Solovay and Strassen (it does not involve the computation of the Jacobi symbol $\left(\frac{a}{m}\right)$ but though the probability of error is the same in the worst case, both conclusions "composite" and "prime" may be incorrect, whereas in Solovay and Strassen's method the conclusion "composite" is always totally reliable.

Acknowledgments. Conversations with Dennis Estes and Sidney Graham are gratefully acknowledged.

REFERENCES

[1] GARY L. MILLER, *Riemann's hypothesis and tests for primality*, Proc. 7th Annual ACM Symposium on the Theory of Computing, 1975, pp. 234–239.

[2] HUGH L. MONTGOMERY, *Topics in multiplicative number theory*, Lecture Notes in Mathematics 227 Springer, New York, 1971.

[3] MICHAEL O. RABIN, *Probabilistic algorithms*, in Algorithms and Complexity, New Directions and Recent Results, J. F. Traub, ed., Academic Press, New York, 1976.

[4] R. SOLOVAY AND V. STRASSEN, *A fast Monte-Carlo test for primality*, this Journal, 6 (1977) pp. 84–85; erratum, 7 (1978), p. 118.

[5] J. VÉLU, *Tests for primality under the Riemann hypothesis*, SIGACT News, 10, 2 (1978), pp. 58–59.